Legal Services Team

Vice-Chancellor's Office
Ellison Building
Newcastle upon Tyne
NE1 8ST
*Tel* 0191 227 4010

1st December 2017

OUR REFERENCE: FOI/RFI-1905/Persson

Dear Ms Persson,

Your request for information received on 2nd November 2017 has now been considered. The response to your request is as follows:

With regards to the Using Student Data for Learning Analytics made reference to in this online policy, https://www.northumbria.ac.uk/-/media/corporate-website/new-sitecore-gallery/services/academic-registry/documents/qte/student-engagement/policy-on-ethical-use-of-student-data-for-learning-analytics-for-internet.pdf?la=en&hash=7BCD0B96D51BB19C2AB16A0ACAC0782867964985 please can you provide the following information in line with the Freedom of Information Act:

**Response**

Northumbria University is currently piloting a small-scale implementation of a Learning Analytics system within one Academic department.

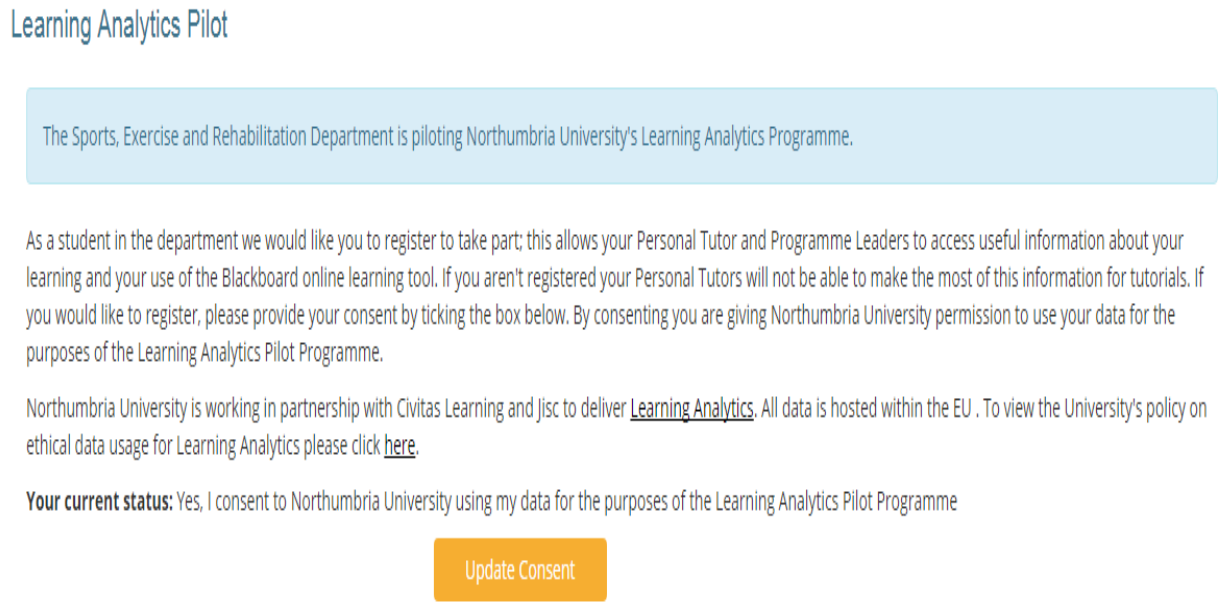
The pilot began in September 2017 and involves a small cohort of students in order to evaluate its potential, to evaluate feasibility and effectiveness and to inform the University as to whether a full scale deployment would benefit students in the future.

The following responses are therefore based on the pilot project - not an "enterprise level" deployment of the technology.

**a) The privacy policy given to students and information around how / when this is explained.**

The project is being piloted within the 'Sports Exercise and Rehabilitation Department' on a student 'Opt-in' basis.

Students on these programmes were asked at enrolment whether they would like to participate in the project and a consent form was presented during their online enrolment (*See below)* which links to the Policy on ethical use of student data for Learning Analytics which defines the use of student data, including the policy not to process sensitive personal data.




Anonymised historical data has been used for the purpose of providing comparable data to evaluate the 'opt-in' cohort against.

**b) the code of conduct given to staff**

Information not held.

For the duration of the pilot project, only one member of staff is analysing a limited amount of data in order to evaluate the Learning Analytics Mechanism. For example, they are using the data collected in order to cross check against any withdrawals from the participating programmes, so as to evaluate whether an intervention may have prevented the students withdrawal.

Should Northumbria University determine from the pilot project that a Learning Analytics tool is something we wish to utilise as part of our Learning and Teaching technology, a "code of conduct" will be developed, informed by the experience of this trial, and provided to all staff with access to the system.

**c) volume of staff with which staff permission levels as listed in 1.2.3. How many staff have access to how many students' data ie 10 staff can access 1000 students, 3 staff can access 10,000, the IT manager has system wide access to X number and which level of data viewing, and entry**

For the purpose of this trial, 3 staff were trained on how to access the limited data of 407 students participating in the trial, however only one member of staff is actively analysing the data collected.

The following is as an example of the level of access provided. Please note that 'student ID's' have been redacted from this snapshot for data protection purposes.


**d) a list of the fields of data items captured in the system used ie name, address, ethncity etc**

As previously stated, Northumbria University is currently running a pilot deployment so to evaluate and inform what a system of this nature can achieve and to allow Northumbria University to use the outcome to develop potential future Learning and Teaching strategy.

Due to the potential competitive advantage a Learning Analytics system could provide to the University should the pilot lead to a full deployment the requested information is withheld because it falls under the exemption in Section 43 of the Freedom of Information Act relating to Commercial Interests.

**43 Commercial interests.**

> *"(2) Information is exempt information if its disclosure under this Act would, or would be likely to; prejudice the commercial interests of any person (including the public authority holding it)"*

This exemption applies because the University considers that the release of such information at this stage of the pilot could prejudice its own commercial interests.

Commercial interests relate to the University's ability to participate successfully in a commercial activity. This could be the ability to buy or sell goods or services or any disclosure that might be deemed information advantageous to market competitors.

The UK Government has stated that the Higher education sector should be a highly competitive market where Universities are in competition with each other to offer the best possible 'product' to existing and potential students and the wider public.

Emerging technologies are one of the means by which such competition can be achieved, meaning that the requested information is considered sensitive because it currently being used to evaluate whether such a technology should be adopted.

Learning Analytics is an emerging technology within the UK Higher Education Sector and we know that as many as 20 other Universities are currently looking at how it can be used to gain a competitive advantage through utilising this technology.

As there are no defined 'must have' data fields in a Learning Analytics system, Northumbria University has selected the data fields that we think will best inform the effectiveness of Learning Analytics. These field may or may not deliver a successful pilot.

Other Universities will or will have chosen their own data fields which may or may not match those used by Northumbria.

To publicise what data Northumbria believes might be used to deliver a successful learning analytics system could give competitors an insight into any potential enterprise deployment of a system, meaning that it would not be in Northumbria's interest for the information to be publically reported at this time.

Because this is a qualified exemption under the Act, Northumbria University has had to balance the public interest in withholding the information against the public interest in disclosing it. The factors considered when deciding where the public interest lay include:

**Public Interest Test**

**The factors considered when deciding where the public interest lay include:**

- There is a presumption of a general public interest in the disclosure of this information.
- There is an interest in ensuring that Data Subjects are informed as to the nature of the processing of their data, particularly any sensitive personal data.

**The reasons for determining that the public interest favours withholding the information are:**

- The timing of the request coming as it does at during a system pilot, not under a full deployment.
- The Policy on ethical use of student data for Learning Analytics already informs the data subjects participating in the trial of the omission of any sensitive personal data.

- The University operates in a global market and faces growing competition from a range of providers. The retention of students, and the ability to assess the potential of any technology that would assist this, is a clear commercial interest.

We therefore conclude that the Public Interest lies in withholding this information.

**e) the (redacted for commercial sensitivities) agreement signed with the system provider on issues such as data management, retention, access, use and purposes, storage location, in event of company sale**

Please find attached the redacted agreement. In addition to your request for Commercially Sensitive Information to be redacted Under Section 43, data which is deemed to be personally identifiable, namely the details of signatories have also been redacted under Section 40 Personal Data. The exemption under section 40 states:

***"Section 40 (2)*** *Personal information.*

*(1)Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject.*

*(2)Any information to which a request for information relates is also exempt information if—*

*(a)it constitutes personal data which do not fall within subsection (1), and*

*(b)either the first or the second condition below is satisfied.*

***Section 40 (3) Personal Information***
*in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the disclosure of the information to a member of the public otherwise than under this Act would contravene—*

*any of the data protection principles, or*

*(ii)section 10 of that Act (right to prevent processing likely to cause damage or distress)"*

Disclosure of this information to the public would not be consistent with data protection principles in the Data Protection Act 1998 (DPA).

Section 40 is an absolute exemption and is therefore not subject to the public interest test.

**Section 43 – Commercial Interests**

As per your request, the agreement has been redacted to remove any “commercial sensitivities”.

**The factors considered when deciding where the public interest lay include:**

- There is a presumption of a general public interest in the disclosure of this information to show that the University has appropriate controls in place when processing personal data.

**The reasons for determining that the public interest favours withholding the information are:**

- The proprietary nature of the redacted content, which may provide the system suppliers competitors with an insight into their business solutions.
- Disclosure of specific security arrangements could provide individuals with dishonest intentions an insight into the supplier’s security arrangements, compromising the interests of both the Supplier and the University.

We therefore conclude that the Public Interest lies in withholding this information.

**f) any profiling algorithm as a schematic**

Information not held.

Northumbria University does not hold a copy of any algorithms being used in this pilot.

**g) a copy of the Privacy Impact Assessment and as listed in 1.4 "notification to the ICO"**

Information not held.

- Privacy Impact Assessments (PIA) are not mandatory under the Data Protection Act 1998.
- Due to the limited scope of the pilot, both in terms of ‘active participants’ and the level of “identifiable data” being used (no sensitive personal data, anonymised data), the University determined that a PIA would not be undertaken for the pilot stage.
- If Northumbria University determines from the pilot that Learning Analytics is a tool we wish to utilise, a full Privacy Impact Assessment will be undertaken, informed in part by the experience of the pilot.

**21 Information accessible to applicant by other means.**

(1) Information which is reasonably accessible to the applicant otherwise than under section 1 is exempt information.

(2) For the purposes of subsection (1)—

(a)information may be reasonably accessible to the applicant even though it is accessible only on payment, and

(b)information is to be taken to be reasonably accessible to the applicant if it is information which the public authority or any other person is obliged by or under any enactment to communicate (otherwise than by making the information available for inspection) to members of the public on request, whether free of charge or on payment.

Northumbria University's ICO notification is published here https://ico.org.uk/ESDWebPages/Entry/Z7674926

If you are unhappy with our response or the way your request has been handled, you have the right to ask for an internal review. To request a review, please contact the Records and Information Manager, in writing at the above address or via email. The review would be undertaken by Jay Wilson, the University's Head of Legal.

Please remember to quote the reference number above in any future communications.

Should you remain dissatisfied following an internal review, you may then appeal to the Information Commissioner at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 01625 545 700

Yours sincerely

Nick Batson

Information Governance Rights Coordinator

**CIVITAS LEARNING INTERNATIONAL LIMITED**
**MASTER SERVICES AGREEMENT**

This Master Services Agreement ("**Agreement**") between Civitas Learning International Limited with company number 07331429 with registered offices at 14-16 Great Chapel Street, Great Chapel street, London, W1F 8FR ("**Company**"), and University of Northumbria, Sutherland Building, College Street, Newcastle upon Tyne, NE1 8ST ("**Customer**"), is entered into and effective as of the date of execution by both parties.

**1. Provision of Services**. Subject to the terms and conditions of this Agreement, including without limitation Customer's payment of all of the fees due hereunder, Company will provide Customer with web-based access to the Civitas databases and applications containing unique and/or personally identifiable information about Customer's faculty, administrators, advisors and students (the "**Platform**") and the cross-institutional database of anonymized information used to provide benchmarking data and other insights (the "**Civitas Learning Network**" or "**CLN**"), together with certain ancillary services provided by Company as may be described in one or more schedules that describe the services (collectively the "**Services**" which are set out in more detail at Exhibit B) together with the pricing and other terms and conditions (each a "**Schedule**"). The Services will be provided for the applicable term set forth in the respective Schedule. Customer may use the Services solely for their intended purpose in accordance with this Agreement.

**2. Customer Responsibilities**. Customer is responsible for all user activities that occur under the Customer's user accounts. Customer shall: (i) have sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of all Customer Data; (ii) comply with all applicable laws of England and Wales and the European Union and any other laws or regulations, regulatory policies, guidelines or industry codes in using the Services ("**Applicable Law**"); and (iii) if and to the extent required in order for Company to perform the Services, Customer will provide Company with access to certain proprietary and third party systems or software where it is permitted to do so pursuant to relevant software licensing agreements. Customer shall use commercially reasonable efforts to obtain the necessary permissions.

**3. Fees and Payment.** Customer shall pay Company the fees in Pounds Sterling and as of the date set forth in each Schedule. Customer shall submit such payments as required in accordance with the payment instructions provided in each invoice. All fees charged for Services are exclusive of all taxes and similar fees now in force, enacted or imposed in the future on the transaction and/or the delivery of Services, all of which Customer will be responsible for and will pay in full, except for taxes based solely on Company's net income. If payment is not made within 30 days' net monthly account after the Company's invoice due date, Company may charge Customer interest on the unpaid balance at the lesser of 1% per month or the maximum lawful rate permitted by Applicable Law, rounded to the next highest whole month and compounded monthly.

**4. Data**. Customer owns all right, title and interest in and is responsible for any data that is collected by Company from Customer or third parties acting on Customer's behalf in connection with Customer's use of the Services ("Data"). Customer grants to Company a perpetual, non-exclusive, royalty-free license to use such Data: (a) in order to provide the Services to Customer; (b) for statistical, analytical and other aggregate use (provided that such Data is not personally identifiable or attributed to Customer and provided that such Data are aggregated with the data from other Company customers or users in a manner that does not allow Customer's Data to be separated from the aggregate data and identified as relating to Customer (collectively, "Blind Data")); and (c) as necessary to monitor and improve the Services. Upon request by Customer, Company will provide Customer with an electronic copy of all Customer Data under Company's control.

All right, title, and interest in and to the Services and associated technology and documentation, including any improvements, modifications, and enhancements made thereto, are and shall remain in Company. Except for those rights expressly granted herein, no other rights are granted, either express or implied, to Customer hereby.

**5. Personal Data.** Within this Section 5, "**Data Controller**", "**Data Processor**", "**Data Subject**", "**Personal Data**" and "**Processing**" shall have the same meanings as in the Data Protection Act 1998 as amended or replaced ("**DPA**") and "Processed" and "Process" shall be construed in accordance with the definition of Processing.

Where Personal Data relating to a Data Subject is Processed by Company (for the purpose of this Section defined as the "Data Processor") or its agents, sub-contractors or staff under or in connection with this Agreement as a Data Processor on the Customer's behalf (for the purpose of this Section the Customer is defined as the "Data Controller"), Company shall

and shall procure that its agents, staff shall:

(a) only Process the Personal Data in accordance with the Data Controller's instructions, which may be specific instructions or instructions of a general nature as set out in this Agreement or as otherwise notified by the Data Controller to the Data Processor from time to time and only to the extent reasonably required in connection with the provision of the Services;

(b) implement and evidence appropriate technical and organisational measures to protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from unauthorised or unlawful Processing or accidental loss, destruction or damage to Personal Data and to the nature of the Personal Data which is to be protected; and

(d) cooperate as reasonably requested by Data Controller to enable Data Controller to comply with any exercise of rights by a Data Subject under the DPA in respect of Personal Data processed by the Data Processor under this Agreement or comply with any assessment, enquiry, notice or investigation under the DPA which shall include the provision of all data requested by Data Controller within 10 Business Days (a Business Day being any day (other than a Saturday or Sunday) on which banks are open for business in the City of London) specified by Data Controller in each case.

(e) ensure that Personal Data will only be transferred or stored within the European Economic Area; provided that Company may transfer Personal Data to its parent company, Civitas Learning, Inc., but only pursuant to Standard Contractual Clauses (or "model clauses") approved by a decision of the European Commission as attached at Schedule 1, Exhibit D. The parties agree that the Customer may review the effectiveness of these clauses in the event that there is any change in data protection law in the United Kingdom or if the European Commission updates or revises the Standard Contractual Clauses.

(f) fully notify the Customer in writing within one Business Day if any Personal Data has been disclosed in non-compliance with this clause 5.

(g) at all times comply with the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Tele-communications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to Processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner ("the Data Protection Legislation").

(g) take reasonable steps to avoid knowingly or negligently doing or omitting to do anything which places the Customer in breach of the Customer's obligations under Data Protection Legislation.

(h) not sub-contract the processing of any Data without the Customer's prior written permission.

(i) The Company will use its reasonable endeavours to assist with any investigation by the Customer or the Information Commissioner's Office (ICO) following a theft or loss under 5(f).

Customer shall rely on the condition of legitimate interest in the DPA to allow it to pass the associated Personal Data to the Company and for the Company to process the Personal Data in accordance with the provisions of this Agreement for Phase 1 Customer undertakes to keep this under review in terms of compliance with DPA and to inform the Company where it considers that the legitimate interest condition no longer applies.

**6. Feedback.** Customer shall provide feedback to Company concerning the functionality and performance of the Services ("**Feedback**") from time to time as reasonably requested by Company. Customer hereby assigns including by way of present assignment of future rights all of its right, title, and interest in and to such Feedback to Company. To the extent that the foregoing assignment is ineffective for whatever reason, Customer hereby grants and agrees to grant to Company a non-exclusive, perpetual, irrevocable, royalty free, worldwide right and licence to use, reproduce, disclose, sublicense, distribute, modify and otherwise exploit such Feedback without restriction.

**7. Warranties.** Company represents and warrants that:

A. Company is the owner or authorized user of the Platform and CLN and all of its components, and to the best of its knowledge the Platform and CLN does not violate any patent, trademark, trade secret, copyright or any other right of ownership of any third party;

B. The Services will perform in accordance with the terms of this Agreement and each Schedule and Exhibit;

C. The Platform and CLN and its components are equipped and/or designed with systems intended to prevent industry known system attacks (e.g., hacker and virus attacks) and unauthorized access to confidential information; and

D. Company will (i) establish and maintain commercially reasonable technical and organizational measures to help to protect against accidental damage to, or destruction, loss, or alteration of Customer's Data; (ii) establish and maintain commercially reasonable technical and organizational measures to help to protect against unauthorized access to the Platform and CLN; (iii) establish and maintain network and internet security procedures, protocols, security gateways and firewalls with respect to the Platform and CLN; and (iv) establish and maintain commercially reasonable disaster recovery plans and (v) will promptly notify Customer if there is any breach of these technical and organizational measures, no later than the next Business Day

Customer represents and warrants that:

A. it has full right, power, and authority to enter into and perform its obligations under this Agreement; and
B. neither the Data nor any other materials provided to Company in connection with the Agreement will infringe, misappropriate or violate any intellectual property, privacy or other right of any person or entity.

Except as set forth herein, the Services are provided "as is" without warranty of any kind, whether express, implied, statutory, or otherwise. Data may be damaged or lost in connection with use of the services. Company specifically disclaims all implied warranties, including those of merchantability, non—interference, accuracy of data, and fitness for a particular purpose.

**8. Indemnity.** Company shall defend and indemnify the Customer against all third party claims, actions, and proceedings, and all liabilities, costs, expenses, damages, losses (including any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties (including those issued by the ICO) and legal and other reasonable professional costs and expenses) awarded or paid in settlement of such claims arising out of or relating to the breach, actual or alleged, by Company of the warranties set forth in Section 6 and the breach, actual or alleged of any other provision of this Agreement or any Schedule. Customer shall defend and indemnify the Company against all third party claims, actions, and proceedings, and all liabilities, costs, expenses, damages and losses (including any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal and other reasonable professional costs and expenses) awarded or paid in settlement of such claims arising out of or relating to i) Customer Data (except where related to the Company's default) or ii) the breach, actual or alleged, by Customer of this Agreement or any Schedule.

Should the Services or any portion thereof become, or in Company's opinion be likely to become, the subject of a claim for which indemnity is provided under this Section, Company shall, as Customer's sole and exclusive remedy, elect in its sole discretion to (i) obtain for Customer the right to use the Services; (ii) replace or modify the Services so that they become non-—infringing provided that such modification does not adversely affect the functional capabilities of the Service as set out herein or the Schedule in which case the Customer shall be entitled to terminate this Agreement and receive a pro-rata refund of any fees paid; or (iii) terminate this Agreement and refund the fees prepaid by Customer for the Services which were not rendered by the Company.

Each party's indemnification obligations hereunder shall be subject to: (i) receiving prompt written notice of the existence of any claim, except that any failure to provide this notice promptly only relieves the indemnifying party of its responsibility pursuant to this Section 7 to the extent its defence is prejudiced by the delay; (ii) being able to, at its option, control the

defence of such claim; (iii) permitting the indemnified party to participate in the defence of any claim at the cost of the indemnified party; and (iv) receiving reasonable cooperation of the indemnified party (at the cost of the indemnifying party) in the defence thereof. If the indemnifying party, within a reasonable time after notice of any third party claim, fails to defend the claim actively and in good faith, i) the indemnified party will (upon further notice) have the right to undertake the defense, compromise or settlement of the claim or consent to the entry of a judgment with respect to the claim, on behalf of and for the account and risk of the indemnifying party, and the indemnifying party will thereafter have no right to challenge the indemnified party's defense, compromise, settlement or consent to judgment and ii) the indemnifying party will promptly reimburse the indemnified party for all reasonable attorneys' fees and costs as they are incurred.

**9. Limitation of Liability.** Except for its indemnity obligations set forth herein, in no event shall either party's aggregate liability arising out of or related to this Agreement, whether in contract, tort or under any other theory of liability, exceed the amounts actually paid by or due from Customer for the Services under this Agreement in the 12 months prior to the event giving rise to liability.

**10. Exclusion of Consequential and Related Damages.** Except for its indemnity obligations set forth herein, in no event shall Company have any liability for any lost profits, loss of data, loss of use, costs of procurement of substitute services, or for any indirect, special, incidental, punitive, or consequential damages however caused and, whether in contract, tort or under any other theory of liability, whether or not Customer has been advised of the possibility of such damage.

**11. Term and Termination.** This Agreement shall remain in effect so long as any Schedule remains in effect. If the Agreement terminates as a result of there being no active Schedule, the Agreement will automatically become effective again in the event that a new Schedule is entered into by and between the parties. In addition to any other remedies it may have, if either party breaches any of the terms or conditions of this Agreement or any Schedule and fails to cure such breach within 30 days after written notice from the non-breaching party, the non-breaching party may terminate this Agreement or a specific Schedule upon 10 days' written notice. Upon termination by the Customer (as a non-breaching party), the Company shall refund any prepaid fees to the Customer covering the remainder of the Term.

In the event that any material change in any Applicable Law, or in the interpretation of such Applicable Law, makes continued performance by any party under the then-current terms and conditions of any Schedule illegal and the parties, using their reasonable best efforts, are unable to agree upon modifications to the Schedule to avoid such illegality, then any party may terminate such Schedule, without penalty, by written notice to the other party, which notice will be effective upon the earlier to occur of (i) the 90$^{th}$ day following delivery of the notice to the other party or
(ii) the effective date of such change in Applicable Law. To be effective, any written notice terminating a Schedule pursuant to this Section must include a detailed explanation and evidence of the illegality created as a result of such change in Applicable Law.

Upon termination of this Agreement for any reason, the Company will provide transition services to facilitate the orderly and complete transfer of Customer Data to the Customer or to any replacement provider designated by the Customer without disruption to the Customer's business ("Transition Services"). The scope and fees of the Transition Services will be mutually agreed to by the parties at the time of termination and the Company daily rate shall be as specified in the most recent Schedule.

Upon the Customer's request within 60 days after the effective date termination of this Agreement, Company will transfer all Customer Data at no charge to portable data mediums (such medium to be approved by the Customer in advance) and surrender these to the Customer. After such period of 60 days, the Company shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, delete all Customer Data in its systems or otherwise in its possession or under its control; provided that Company has no obligation to delete any Blind Data.

**12. Confidential Information.** Customer acknowledges that the Services, the Platform, the CLN, the terms of this Agreement, and any other proprietary or confidential information provided to Customer by Company (**"Company Confidential Information"**) constitutes valuable proprietary information and trade secrets of Company. Company acknowledges that any proprietary or confidential information provided to Company by Customer (**"Customer Confidential Information"**) constitutes valuable proprietary information and trade secrets of Customer. Each party agrees to preserve the confidential nature of the other party's Confidential Information by retaining and using the Confidential Information in trust and

confidence, solely for its internal use, and by using the same degree of protection that such party uses to protect similar proprietary and confidential information, but in no event less than reasonable care. Each party shall have the right to apply for an injunction to prevent any breach or continued breach of this section. Each receiving party agrees to promptly report any breaches of this section to the disclosing party.

Notwithstanding the foregoing, Confidential Information shall not include any information which (i) is now, or hereafter becomes, through no act or failure to act on the part of the receiving party, generally known or available to the public without breach of this Agreement by the receiving party; (ii) was acquired by the receiving party without restriction as to use or disclosure before receiving such information from the disclosing party, as shown by the receiving party's files and records immediately prior to the time of disclosure; (iii) is obtained by the receiving party without restriction as to use or disclosure by a third party authorized to make such disclosure; or (iv) is independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information, as shown by documents and other competent evidence in the receiving party's possession.

Each party agrees that the terms relating to price, payment and fees under this Agreement and any Schedule are confidential. In the event that Customer receives any request under the Freedom of Information Act 2000 ("FOIA") or any other Applicable Law for disclosure of any information within or relating to this Agreement or any Schedule, it undertakes to: (a) notify the Company as soon as practicable of the details of the request; and (b) assert to the fullest extent of the law any available exemptions to prevent the requested disclosure including but not limited to sections 36, 41 and 43 of FOIA. The Customer will be responsible for determining in its absolute discretion and notwithstanding any other provision in this Agreement, whether any information is exempt from disclosure in accordance with the FOIA.

**13. Force Majeure.** Neither party will be liable for any failure or delay in its performance under this Agreement due to any cause beyond its reasonable control, including acts of war, acts of God, terrorism, earthquake, flood, embargo, riot, sabotage, labour shortage or dispute, governmental act, or failure of the Internet (not resulting from the actions or omissions of Company), provided that the delayed party: (i) gives the other party prompt notice of such cause, and (ii) uses its reasonable commercial efforts to promptly correct such failure or delay in performance. Notwithstanding the foregoing provisions of this Section 13, Force Majeure shall not include the non-availability or lack of funds or failure to pay money when due, except for failure to pay money caused by events affecting all reasonable means of payment, in which event, on the cessation of such event, Customer shall pay the amounts due hereunder. If Company is unable to provide Services for a period of 30 consecutive calendar days as a result of a continuing force majeure event, Customer may cancel the Services upon written notice to Company and the Company shall refund any prepaid fees to the Customer covering the remainder of the Term.

**14. Publicity.** Company may reproduce and display Customer's logos, trademarks, trade names and similar identifying material in Company's marketing materials (such as in press releases and on Company's website) for the purpose of referring to Customer as a customer of Company. In addition, Customer shall issue a joint press release with Company, participate in a Company case study, and participate in analyst calls requested by Company. The content of any press release and case study shall be subject to Customer's prior written approval, which shall not be unreasonably withheld, conditioned or delayed.

**15. Assignment.** Either party may assign this Agreement in connection with a merger, acquisition or sale of all or substantially all of its assets related hereto. Except as expressly stated in this Section 15, neither party may assign its rights or obligations under this Agreement without obtaining the other party's prior written consent. Any assignment in contravention of this Section shall be void. On obtaining the Customer's prior written consent, the Company may utilize third parties to host the Platform and assist Company with certain of the Services, provided that the use of a third party will in no way mitigate Company's obligations herein, and Company will be fully liable for any acts or omissions of any third party service provider. Customer hereby consents to Company's use of Amazon Web Services to host the Platform and Customer Data.

**16. Independent Contractor.** In performing under this Agreement, each party is acting as independent contractor, and in no way are the parties to be construed as partners, joint venturers, or agents of one another in any respect.

**17. Governing Law and Jurisdiction.** This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England and Wales and each party irrevocably agrees that the courts of England and Wales

shall have exclusive jurisdiction to settle any such dispute or claim.

**18. Notices.** All notices and other communications required or permitted under this Agreement shall be in writing and delivered: (i) personally; (ii) by first class mail; or (iii) via a recognized courier, to the applicable Party at the addresses set forth below, unless, by notice, a Party changes or supplements the addressee and addresses for giving notice. All notices shall be deemed given on the date personally delivered or 5 days after deposit in the mail as specified.

19. The Company shall procure the execution and delivery to the Customer by its parent company within 7 days of a written request from the Customer in the form set out in Schedule 2 to this Agreement with only such amendments as the Customer may approve.

20. If there is an inconsistency between any of the provisions of this Agreement and the provisions of Schedule 1, Exhibit D, the provisions of Schedule1, Exhibit D shall prevail.

| If to Customer: | If to Company: |
|---|---|
| **Accounting Contact:** Chief Operating Officer | **Address:** |
| | Civitas Learning International Limited |
| | Attention: CFO |
| **Address:** University of Northumbria at Newcastle | 100 Congress Avenue, Suite 300 |
| Sutherland Building | Austin, TX 78701 |
| College Street | **Telephone:** (512) 215-9628 |
| Newcastle upon Tyne, NE1 8ST, U.K | |
| **Telephone:** (0044) 191 2274006 | |

**19. Miscellaneous.** This Agreement, including the exhibits attached hereto, constitutes the entire agreement between the parties regarding the subject matter stated herein, and supersedes all previous communications, representations, understandings, and agreements, either oral, electronic, or written. Each party agrees that it shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement. Each party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in this Agreement.

Any amendments to this Agreement shall only be valid if in writing and signed by an executive of both parties. Nothing contained in any purchase order or other document shall in any way modify this Agreement or add any additional terms or conditions. This Agreement may be executed in two counterparts.

**20. Anti-slavery and anti-bribery**

In performing their obligations under this Agreement the parties shall take steps to ensure that there is no slavery, human trafficking, bribery or corruption in their business or its supply chains and that they and each of their subcontractors shall comply with all applicable laws, statutes, regulations and codes from time to time in force including but not limited to the Modern Slavery Act 2015 and Bribery Act 2010.

| CUSTOMER |
| --- |
| Section 40 [redacted] |

| CIVITAS LEARNING INTERNATIONAL LIMITED |
| --- |
| Section 40 [redacted] |

# CIVITAS LEARNING INTERNATIONAL LIMITED
# SCHEDULE 1

| | |
|---|---|
| **Civitas Learning International Limited** | **University of Northumbria at Newcastle** |
| **14-16 Great Chapel Street, London, W1F 8FR** | **Sutherland Building** |
| **Attention: Scott Chamberlain** | **College Street** |
| | **Newcastle Upon Tyne, NE1 8ST** |
| | **Attention: Chief Operating Officer** |

**Effective Date**: 1 June 2017

This Schedule incorporates and is subject to the Master Services Agreement (the "MSA") between Civitas Learning International Limited ("**Company**") and the Customer identified above dated May 17, 2017. This Schedule describes, among other things, the services to be provided to Customer by Company. To the extent of a conflict between this Schedule and the MSA, this Schedule shall control. Unless otherwise provided herein, capitalized terms shall have the meanings provided in the MSA.

A. **Company Responsibilities**: Company will:

1. establish and maintain a private, secure, restricted-access instance of the Civitas Platform for Customer, granting access only to members of Customer and Company's staff as jointly and unanimously designated by Customer's authorized administrators;
2. integrate the systems listed in Section D with the Civitas Platform (new or replacement integrations subject to additional fees);
3. provide Customer with access to the following Platform applications:
    - **Illume Students Insights Platform**
4. provide Customer periodic CLN Reports, when available;
5. provide the services as listed in Exhibit B

Upon implementation, the Civitas Platform will be made available in accordance with the service level agreement attached to this Schedule as Exhibit A.

B. **Customer Responsibilities**: Customer shall:

1. follow an agreed upon schedule and project plan for integration efforts;
2. Section 43 [redacted] and read-only user account(s) for Company to access the historic and current data in Customer's systems listed in Section D below, on a mutually agreed schedule;
3. assign a project manager and provide Company with access to the relevant functional, technical and business resources with adequate skills and knowledge to support the performance of Services;
4. obtain any consents and access to data or rely on the legitimate interest condition set out in the DPA, at Customer's sole expense, required for Company to perform Services;
5. where reasonable and at its sole discretion provide information regarding Customer's business policy, processes and its organization sufficient to support Company's delivery of Services and applications described in this Schedule;

6. acquire and set-up, install and provide maintenance of the required hardware and network environments to facilitate delivery of Services.

C. **Term:** This Schedule is effective as of the Effective Date and will remain in effect for 1-year, unless terminated earlier pursuant to the MSA.

D. **Fees:** Customer shall pay the one-time platform and subscription fee set forth below, which the Company may invoice upon the Effective Date. Customer shall pay Company the annual subscription fee(s) set forth below, which is payable in advance for the Term of this Schedule, beginning upon the Effective Date. Company may invoice Customer the integration and/or consulting block fees upon Customer's request for integration and/or consulting services. Customer shall also reimburse Company all reasonable actual expenses incurred by Company for travel-related expenditures that are required to successfully deliver against the obligations under this Schedule. Such expenditure shall comply with the Customer's travel and expenditure policy at Exhibit C.

| | | |
|---|---|---|
| **ANNUAL SUBSCRIPTION FEES** | Annual Subscription fees include the following: 43 [redacted] | |
| | 43 [redacted] | |
| **IMPLEMENTATION FEES** | 43 [redacted] | |
| | 43 [redacted] | 43 [redacted] |
| Consulting Fees *(if applicable)* | | N/A |
| New or Replacement System Integrations | | TBD per integration scoping |

**ACCEPTED AND AGREED:**

| **Company** | **Customer** |
|---|---|
| **Civitas Learning International Limited** | **University of Northumbria at Newcastle** |
| Section 40 [redacted] | Section 40 [redacted] |

## EXHIBIT A
## Service Level Agreement

1. **Definitions**
   - 1.1. "Commercially Reasonable Efforts" means the same degree of priority and diligence with which the Company meets the support needs of its other similar customers.
   - 1.2. "Failure Event" means a period of Unavailability in excess of 5 minutes.
   - 1.3. "Fault" means any failure of the Civitas Platform to operate in all material respects in accordance with the specification outlined in Exhibit B including any failure or error referred to in the Service Level Table
   - 1.4. "Helpdesk Support" means any support provided by help desk technicians sufficiently qualified and experienced to identify and resolve most support issues relating to the Civitas Platform.
   - 1.5. "Maintenance Window" means a period scheduled by Company during minimal traffic times, not to exceed 2 hours per week, wherein Company can perform maintenance tasks.
   - 1.6. "Service Levels" means the service level responses set out in the Service Level Table
   - 1.7. "Solution" means the correction of a Fault or a workaround in relation to a Fault that is reasonably acceptable to the Customer.
   - 1.8. "Support Request" means a request made by the Customer in accordance with this Service Level Agreement for support in relation to the Civitas Platform
   - 1.9. "Support Services" means the maintenance of the Civitas Platform including Help Desk Support
   - 1.10. "Unavailability" means the Civitas Platform is unavailable outside the Maintenance Window.
   - 1.11. "Uptime" means the general availability of the production instance of the Civitas Platform. Uptime will be measured by a calendar month period and calculated as follows: (total minutes in any calendar month – total minutes of Unavailability) divided by (the total minutes in same calendar month).

2. **Uptime Commitment.** Company will deliver 99% Uptime for the Civitas Platform.
   - 2.1. Exceptions. Company is not responsible for a failure to meet any Service Level to the extent that failure is attributable to any of the following, in which case the services downtime or Failure Event does not count against the Uptime commitment:
     - 2.1.1. Customer's failure to perform any of its responsibilities set forth in the Agreement to the extent such failure adversely affects Company's ability to meet the Uptime commitment.
     - 2.1.2. Factors outside Company's reasonable control; provided that Company would have been able to perform but for such factor, Company has not materially contributed in the cause of such factor, and Company could not have reasonably foreseen and prevented the effect of such factor with a commercially reasonable effort.

3. **Support Services.**
   - 3.1. During the Term, the Supplier shall perform the maintenance of the Civitas Platform during regular business hours with the exception of the Maintenance Window ("the Support Services").
   - 3.2. The Customer may request Support Services by way of a Support Request.
   - 3.3. The Company shall provide Help Desk Support by means of the following email addresses UK-Team@civitaslearning.com or UK-team@civitaslearning.co.uk;
   - 3.4. The provision of Support Services shall be included within the Annual Subscription Fees for the duration of the Term

4. **Service Levels**
   - 4.1. The Company shall prioritise all Support Requests based on its reasonable assessment of the severity level of the problem reported and respond to all Support Requests in accordance with the responses and response times specified in the table set out below:

Section 43

[redacted]

4.2. The parties may, on a case-by-case basis, agree in writing to a reasonable extension of the Service Level response times.

4.3. The Company shall give the Customer regular updates of the nature and status of its efforts to correct any Fault or Failure Event.

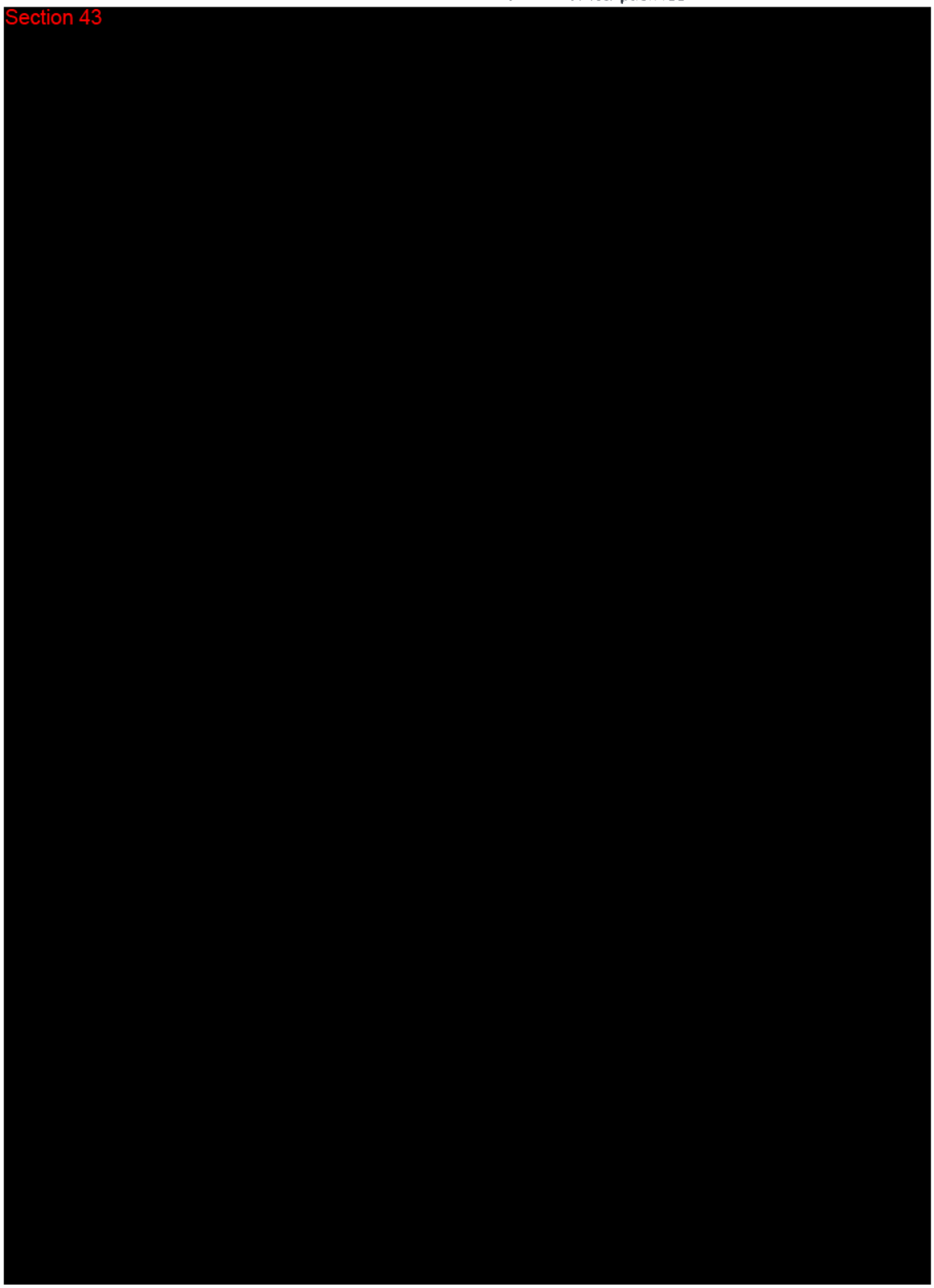
5. **Communication.** In the case of a Failure Event or Fault, Company shall use commercially reasonable efforts to (i) notify Customer's designated contact, (ii) identify the source, and (iii) resolve.

6. **Termination Option.** Failure for Company to meet the Uptime commitment during 2 consecutive calendar months shall constitute a material breach of this Schedule and Customer may terminate this Schedule with 30 days written notice without opportunity to cure. The provisions of this Exhibit A state Customer's sole and exclusive remedy for any Uptime failures of any kind. Upon termination pursuant to this section 6, the Customer will receive a pro-rata refund of fees paid for Services applicable to the period from the effective date of written notice to the end of the then current annual term.

**EXHIBIT B**

**The Services to be included within the annual subscription fee**

Section 43



Section 43

| TABLE 1 | 2017 | | | | | | | 2018 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Activity | Jun | Jul | Aug | Sep | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May |
| **Phase 1: Data ingestion (SITS and Blackboard) of historical information (anonymised), train models and test** | | | | | | | | | | | | |
| Kick Off Meeting | | | | | | | | | | | | |
| Ingest data sources into Civitas system | | | | | | | | | | | | |
| Validate data and enable data science | | | | | | | | | | | | |
| Assist Customer with generating reports on key predictive variables | | | | | | | | | | | | |
| Develop student success action plan | | | | | | | | | | | | |
| Training and empowerment of users on the system | | | | | | | | | | | | |
| **Phase 2: Apply insight from historical data to live data in the pilot population** | | | | | | | | | | | | |
| Ingest live data nightly | | | | | | | | | | | | |
| Implement Student Success Action Plan | | | | | | | | | | | | |
| Provide ongoing support for users to access information via the system | | | | | | | | | | | | |
| Continue to empower users throughout live period | | | | | | | | | | | | |
| Assist Customer with generating final report of project including availability statistics | | | | | | | | | | | | |

**EXHIBIT C**
**TRAVEL AND EXPENDITURE POLICY**

# Travel and Expenditure Policy

## Introduction

The Travel and Expenditure Policy sets out how University employees, students and contractors (referred to as 'the Traveller 'in this policy) should make appropriate and cost effective travel arrangements. The policy has been developed in line with the University's Corporate Strategy 2013-18. Developed on best practice principles, the policy contributes directly towards the University's Corporate Strategy to strengthen operational efficiency and effectiveness and foster a culture of continuous improvement.

### Purpose and Scope

This Policy provides guidance to University Travellers on:

- Booking methods
- Financial authority and approvals
- Reimbursement of travel expenses
- Duty of care
- Risk assessments
- Subsistence or other expenses incurred in connection with University business
- The receipt and provision of business and corporate hospitality
- The use of mobile telephones; and
- Other non-pay expenditures incurred in connection with University business.

### Table of Contents

## General Principles

The University is committed to the 'Nolan' principles as defined by the Committee on Standards in Public Life 1994 - 1997: selflessness; integrity; objectivity; accountability; openness; honesty and leadership.

Effective budgetary control is the responsibility of senior managers across the University. Principal Budget Holders will ensure that expenditure under their control provides value for money (VfM), within the agreed financial budget(s).

It is the responsibility of every claimant and authorised signatory to ensure that University expenditure is necessary, appropriate and proportionate to the activities for which the funding is designated.

This Policy will apply irrespective of the source of funding. The University may withhold payment of any expenses incurred not in accordance with this Policy. It will seek reimbursement of any expenses paid and later found to be invalid.
This section defines the Travel and Expenses Policy, procedures and guidelines for Northumbria University. Travellers undertaking business travel or staying in accommodation are required to adhere to this Policy. Complying with this Policy allows the University to negotiate and make significant savings on all aspects of travel costs.

As part of the University's Duty of Care, the University is required to have knowledge of the location of each member of staff when travelling on business. It is important therefore, that staff comply with the requirements of this Policy, so the University will be able to assist individuals more easily if an emergency situation arises. Moreover, line managers are responsible for ensuring that this Policy is applied within their own area. Failure to comply with the policy may result in disciplinary proceedings.

## Glossary of terms and abbreviations

| | |
|---|---|
| **Authorising Manager** | An authorised signatory is a Principal Budget Holder, Senior Signatory, or Nominated Signatory as defined in paragraph 5 of the Policy. |
| **Budget Holder** | A nominated member of staff who has been given prior consent to authorise a set value of financial money. |
| **CIBT** | The University's approved supplier for visas / global visa's. |
| **CRG** | Control Risk Group at the Foreign and Commonwealth Office |
| **ESTA** | Electronic System for Travel Authorisation |
| **FCO** | Foreign and Commonwealth Office. |
| **ICE** | This is an in case of emergency contact number. |

| | |
|---|---|
| **Lowest priced logical ticket** | This is the lowest priced journey that delivers the traveller to their destination within the timeframe necessary to meet the business need |
| **Restricted Economy Ticket** | This is an airline ticket that has restrictions in place, however in most instances amendments can be made for a fee and the ticket will be non-refundable |
| **TMC** | Travel Management Company, which has been appointed as the University's travel provider. |
| **VfM** | Value for Money |

**Useful Numbers**
CRG: 020 79702100
TMC: 0161 819 7769
Speciality Assist: 0207 902 7405
TMC: 24 Hour Emergency Number: 0207 79602

## Policy aims

The aims of the Policy are:

To provide clear information which supports safe, convenient, comfortable, sustainable and cost effective travel for the University traveller. To reimburse Travellers for reasonable and necessary expenses, which they incur in the authorised conduct of University business.

To help Travellers adhere to the University's reporting and accounting standards.

To support expenditure control using good judgment and the services of nominated travel providers and negotiated discounts, where applicable.

To reduce, where possible, costs to both the University and the impact on the environment it is important in each instance to assess if business travel is necessary.

Video conferencing and telephone conferencing facilities should always be considered before booking any business travel. Travellers are asked to plan and make requests for journeys, accommodation, conferences, training etc. as far in advance as practicable. Advance bookings are considerably cheaper than purchasing nearer to the time of travel and the use of budget airlines can significantly reduce the cost of air travel. These options should be used where possible.

If you have any questions in regard to the Policy or its application, please do not hesitate to contact Human Resources and/or Procurement.

The Policy is in line with the University's Financial Regulations. It applies to all Travellers and to any other person responsible for expenditure on behalf of Northumbria University.
The Chief Operating Officer is responsible for the implementation of this Policy and will arbitrate in any cases of dispute.

The Policy can also be viewed on the travel portal at:
**https://www.northumbria.ac.uk/staff/travelhub/travelfor/?view=Standard**

## Contractors

All contractors working on behalf of Northumbria University need to comply with the content of this policy to ensure that their incurred expenses are reimbursed and wherever possible/reasonable bookings should be made through the TMC.

# 1. Financial Authority and Approvals

## a. Delegated Financial Authority

In order to maintain accountability and transparency, all expenditure should be reviewed, approved and authorised in accordance with the following thresholds:

- For expenditure **up to £50,000 including VAT**, Principal Budget Holders have delegated responsibility. They may also nominate one additional senior signatory to cover for their absence (for example through annual leave, working off campus, travelling overseas).
- For expenditure **up to £25,000 including VAT**, Principal Budget Holders may nominate an additional senior signatory.
- For expenditure **up to £5,000 including VAT,** Principal Budget Holders may delegate responsibility to **any nominated signatory**.
- In accordance with the Financial Regulations, incorporating the Corporate Gifts and Hospitality Policy, a full list of approved signatories will be maintained by Finance and Planning and will be reviewed annually. Any changes between the annual reviews should be notified to the Chief Operating Officer by the Principal Budget Holder.

## b. Corporate Credit Cards

The University operates a Corporate Credit Card Scheme. This scheme is restricted to members of the University's Management Group and regular international travellers. The Company Barclaycard should be used only for the purpose of expenses incurred whist travelling on University business.

All transactions should be substantiated with receipts. The University reserves the right to seek reimbursement for any item of non-receipted expenditure.

Where accommodation costs are paid using a corporate credit card, authorised signatories are required to assess whether such claims are reasonable.

The card user should send a personal cheque to cover personal items with the completed reconciliation form. Cash withdrawals are not permitted, if cash withdrawals are made this will result in action being taken to recover monies.

## 2. Responsibility and Compliance

The University's appointed TMC (refer to Glossary) is contracted to operate within this Policy. Travellers, Principal Budget Holders and nominated signatories are responsible for complying with this Policy. The Principal Budget Holder and any authorised signatory are responsible for accurately reviewing expense reports and exception reports for compliance.

All business travel and accommodation should be booked through the TMC and when appropriate, the online booking tool should be used to comply with University policy and duty of care. All travel arrangements should be discussed with the Traveller's line manager and approved in principle by email prior to contacting the TMC.

While this Policy is comprehensive, it is nevertheless impossible to anticipate every situation that may be encountered by the Traveller in the course of their business travel. All Travellers are expected to exercise good business judgment while travelling on University business.

### a. Risk Assessment

All Travellers are required to conduct an appropriate risk assessment prior to travel. For UK and Europe travel to low and medium risk destinations, a declaration based risk assessment is required prior to booking travel. The university travel provider incorporates this as part of the travel booking process. For travel outside the EU, or where a group booking is being made, a more detailed risk assessment is required. A template for the more detailed risk assessment is stored on the intranet Travel Hub. To identify low/medium/ high/extreme risk categories of destinations (major cities and regions across the world) the traveller will need to check the rating on the Foreign & Commonwealth Office website and that of Control Risks Group. CRG (Control Risk Group) are the University's preferred supplier for risk management. CRG also provides "live" travel alerts and a bespoke travel security service to a designated team of staff across the University. More details can be found on the travel hub.
A standard set of 'controls' for all travellers have been set out on the risk assessment templates. University policy requires these to be adhered to by all staff and students.

### b. Security app for mobile devices

The university has procured mobile security app's for staff and student's use both on campus and during travel. Travellers are required to register with the appointed service provider prior to travel and follow the instructions for

- keeping line management informed of progress
- changes to itineraries
- use should the traveller be personally threatened (e.g. assault, travel accident)

### c. Travel to High or Extreme Risk Countries

For any Travellers travelling to a country ranked by CRG as EXTREME risk they must seek specific approval prior to making any travel arrangements. For any travel to HIGH risk countries all advice and guidance provided by CRG must be adhered to. Approval may be granted following evidence that the Traveller has taken the necessary steps to ensure their travel plans take into account their personal safety. Approval can only be given by designated senior management employees of the University, it is the responsibility of the Traveller and approver to ensure the Traveller's safety at all times.

The Foreign & Commonwealth office define 'essential travel' as: "…. urgent family or business commitments to attend to. Circumstances differ from person to person…. make an informed decision based on the risks."
The university will require a very strong case to be made by any traveller to demonstrate their proposed travel to a specific destination at a specific time is 'essential travel'.

## d. Emergency Situations

Should a serious incident occur whilst the Traveller is travelling on University business, either nationally or internationally, they must:

- When personal safety is threatened, activate the mobile application sanctioned by the university
- In medical emergencies call Specialty Assist (Specialty Group Companies are focused on travel and health to provide medical assistance and claim management services all around the world) who will make arrangements to support getting Travellers home safely
- For emergency travel requirements contact Control Risks Group
- Confirm their situation and wellbeing to their line manager, or, if it is out of hours (09:00-17:30), contact the University's Security Services who would coordinate any major incident, e.g. volcanic ash cloud) on +44 (0) 191 227 3999.

Travellers should be aware that in the event of a serious security incident mobile telephones may not be operable. In this situation, landline telephones should be used. Line Managers or the Security Service will contact family members, if required.
It is also important to store an ICE (In Case of an Emergency) number in your mobile telephone so that should you not be in a position to contact someone yourself, then a third party could do so on your behalf. A good idea is to take a photo of your ICE number and save it as your screensaver on your phone.

## e. Corporate Social Responsibility/Duty of Care

All air, hotel and rail requirements must be booked through the TMC via their online web portal and/or the designated telephone number. Expenses for travel NOT booked via TMC will not be refunded unless mitigating circumstances are supported by the travellers' line manager.

Northumbria University will not send its Travellers to any country where the Foreign and Commonwealth Office has issued a "no travel" alert and will also do everything it possibly can to remove staff from any high alert areas. A link to the Foreign and Commonwealth Office can be found on the online booking tool. Travellers should always check this if considering travel to an international destination for business. Northumbria University has a Duty of Care to its Travellers to ensure that they travel safely.

## f. Insurance

The University's travel insurance covers all travellers on Northumbria University business. Alternative cover is required for a spouse/partner/child if they are accompanying staff on a business trip.

A copy of the policy is available at:-
http://www.northumbria.ac.uk/static/5007/campserv/travelinsurancedoc.pdf

Our insurers appreciate that during business trips, especially overseas, there will be social activities and these are insured for the business period.
Any member of staff wishing to extend their business trip for holidays or to engage in 'hazardous activities'1 during their social hours will need to arrange their own insurance.

1 – Hazardous activities are where a reasonable person would need to make a risk assessment e.g. the activity includes winter sports, bungee jumping, white water rafting.

## 3. Travel Procedure

Travellers must discuss and agree all travel, accommodation (and where necessary) subsistence with their line manager prior to making a booking. Providing Travellers do not exceed the set limits, all travel and accommodation will be pre-approved. If a particular trip exceeds the set limit as displayed on the online booking tool then this will require approval by the appropriate authorised signatory, as clear justification will be required as to why the trip has exceeded the set limit.

### a. Travel Arrangements

Travellers should consider the following before requesting any travel or accommodation.

- Cost of travel and accommodation
- Cost of any support required e.g. translators
- Key events in destination country / city that may disrupt travel or increase costs e.g. festivals, travellers urged to avoid such times if possible
- Time and duration of complete journeys
- Requirement for flexibility within the itinerary
- Alternate options such as video conferencing /Skype / hosting webinars
- Meeting clients and prospective customers (students are legally defined as customers) in safe environments
- Carbon impacts from the mode of travel

Travellers are also expected to consider whether the journey is essential or alternative options, where other Travellers are travelling to the same destination on the same dates for example.

As it is considerably cheaper to book travel online the online booking system should be your preferred method of booking wherever possible. The URL is **www.keytravel.com** only in the case of complex and/or multi sector itineraries should bookings be made via the telephone/email. The University's TMC will redirect you to the online system for simple point-to-point booking, hotel reservations and rail tickets, unless there is a valid business justification for bookings to be undertaken by the TMC.

A reason for travel should be selected from the drop down menu within the online booking platform, any additional information can be added within the free text field, and this additional information will give the approver with more detail on the proposed travel requirement.

For more details on booking travel, please refer to the Key Travel Academy where you will find User Guides and Tips.

## b. Traveller Profiles

All Travellers who undertake business travel on behalf of the University must complete and maintain their traveller profile on the online tool. This information will be held securely by our agent. Once a profile has been submitted only the Traveller and the University's preferred supplier can view it. The Traveller can amend this information at any time through the online traveller profile tool. In a potential crisis situation, the traveller profile will be used to assist the University and its agents. When travelling to countries which require a visa it will also enable TMC to submit passport information which is required at the time of booking.

It is the Traveller's responsibility to ensure they have a valid passport to travel overseas on University business and request the relevant business visa through the TMC. The University will not reimburse Travellers for any costs associated with the issue of an initial passport or renewal of an initial passport. Passports should have a minimum of six months' validity from the date of departure and be machine-readable for entry to the United States. The University will reimburse Travellers for the cost of a second passport should this be required for business reasons (e.g. visa applications for frequent travellers). Approval must be sought from the budget holder. Any questions regarding passport requirements should be directed to the relevant immigration service's website for the country the Traveller intends to visit.

## c. Ticket Delivery

For air travel, the TMC will utilise ticketless/electronic travel where possible. In the event that a paper ticket is issued, this will be sent out by Royal Mail special delivery. Rail travel tickets may be collected from the on-campus ticket printer which is located in the Security Office or from a quick ticket machine at a designated railway station selected at time of booking. Alternatively, these can be posted to a home address if required.

## d. International Travel

For the purposes of this Policy, international travel covers all destinations outside the UK and Ireland. Travellers anticipating travel to international destinations should notify/seek pre-trip approval from their Line Manager at least seven working days prior to the proposed departure date, whenever possible. Foreign countries require a passport and in some instances, a visa.

## e. Visa Service

Go to the Key Travel Visa Database to download visa application forms and obtain information on visas:
**http://www.keytravel.com/uk/products-and-services/visa-services/visa-database/**

Key Travel has an in-house visa team based in their London office.
All staff travelling on University business should obtain the correct relevant visa category, such as business travel visas. All visa applications need to be sent to our London office by secure delivery. Key Travel recommends that you use secure delivery, such as Royal Mail Special Delivery by 1pm, DHL by 12.00 or 9.00 or use a same day courier.

Key Travel
Visa Department
1st Floor
28-32 Britannia Street
London

WC1X 9JF

## f. Immunisation

Travellers should check on the FCO website **https://www.gov.uk/foreign-travel-advice** for up to date vaccination advice, this detail can be found on the travel booking website. Appropriate measures should then be taken to ensure the Traveller is suitably protected. The University's Occupational Health Service can provide advice and support on the required immunisation.

All immunisations required to travel to a country on University business are a reimbursable expense.

## g. Travel booked by a Third Party

Should a Traveller have travel or accommodation booked on their behalf by an external party, and not through the University's TMC, the Traveller should provide a copy of the travel itinerary, and a risk assessment, to their line manager. This is a duty of care requirement and it is the Traveller's responsibility to ensure that this requirement is met.

## h. En Route Changes

If travel plans change when the Traveller has already commenced their journey the TMC can make changes to travel arrangements – contact 0845 2668865 (option 2). In most instances these can be managed through the online booking tool. If it is not possible to access the TMC or it is out of business hours (8.45am to 5.30pm) changes can be made by contacting the 24-hour emergency number 0207 8439602.

The TMC may be able to make changes without further cost to the business; this will be made clear during the call. Wherever possible itinerary changes should be minimised, since changes often result in substantial additional cost to the University.

When abroad, any illness preventing completion of the booked travel must be supported by a doctor's statement to obtain a refund of travel costs via insurance. Emergency situations should always involve contact with Specialty Assist tel: +44(0)20 7902 7405. Disinclination to travel prior to or during the trip is not insured.

## i. Air Travel

### (i) International Travel Schedule

Each Faculty and Service will prepare an annual detailed International Travel Plan and submit it to the International Office. The Plan should include the following detail for each international journey:

- The purpose of the trip and intended outcomes
- Names of all Travellers
- The event they are travelling to, for example conference, research, business development, accreditation
- Date of travel
- Total cost (including best estimate of the cost of travel, hotel, per diem rates and out of pocket expenses)

The International Office will look to consolidate journeys by coordinating travel wherever possible. Once agreed, the Travel Plans will be shared with the TMC, so it can seek to optimise the University's expenditure on international travel.

All air travel requires approval from the line manager before a booking is made. All travel arrangements should be discussed with the Travellers' line manager and approved in principle by email, prior to contacting the TMC.

The air travel booking process has been configured to seek approval from a designated authorised manager/budget holder. Until this approval has been confirmed, no reservation will be confirmed.

Air travel reservations should be made through the online booking tool, where possible.

For more complex or difficult itineraries (known as multi-sector trips, e.g. London – Amsterdam – Dubai – Moscow – Newcastle upon Tyne) bookings should be made by calling the TMC.

Air travel reservations must not be made directly through airlines.
If a flight reservation needs to be booked or amended out of business hours Travellers will need to call the TMC out of hour's service on 0161 3600250.

### (ii) Making a Group Air Reservation

Please call the Key Travel Groups team on 0161 8198935 to make a group air reservation.

### (iii) UK Air Travel

Air travel within the UK should only be used where it represents best value for money. It should therefore only be used if it is cheaper than alternatives taking into account the total cost of the journey including, for example, accommodation costs, or where it is demonstrably more convenient.

All domestic air travel should be ticketed in economy class with restricted economy being the first choice. Where there is more than one airline operating a particular route, Travellers should select the least expensive journey.

### (iv) International Air Travel

All international air travel for flight durations of less than 5 hours should be booked in economy class. Flights of over five hours should normally be booked in Economy Comfort (Premium Economy) and, to minimise the effects of long haul travel, staff are expected to factor into their travel plans a rest and recovery period of eight hours on arrival at their accommodation and prior to attending meetings or commencing work activities. If waits at airports are longer than 90 minutes, and travelling long-haul. airport lounge access may also be booked with Economy Comfort travel This lounge booking should be made via Key Travel. A small number of very frequent travellers will be able to have annual airport lounge access membership cards.

The lowest priced logical airfare should always be booked. Connections, alternative airports and low cost carriers should be utilised where there is a saving to the University that does not impact upon achieving business requirements.

In exceptional circumstances and where appropriate and cost effective, flights over five hours may be booked in Business Class. That is, if the Business Class fare is less than or equal to the combined cost of Economy Comfort plus the additional rest and recovery period (salary, hotel and subsistence) costs, or if a University Occupational Health Assessment indicates that this is necessary in specific individual circumstances. In these circumstances a clear business case for travel should have been

made to – and approved by, a relevant member of the Senior Management Group prior to making the booking. All Business Class travel will be reported to the University Executive on a six monthly basis.

International travel which is not included in the annual international travel schedule should be considered and pre-approved by the relevant line manager and, if not research related, also the International Office.

### (v) Upgrades for Air Travel

Upgrades at the expense of the University are not permitted. Therefore, upgrades must not be requested before a ticket is issued as the University would be charged the cost of the upgrade. Any such requests will be highlighted in a monthly exception report. Travellers making requests for upgrades after a ticket has been issued, do so at their own discretion and must personally cover any additional costs.

### (vi) Cancelling Air Travel

Cancellations should be made through the online booking tool where possible or via the Key Travel Customer Service Team on 0845 2668865 (option 2). It is important to cancel any trip that is no longer required as the airline will reimburse the University with any taxes or fares due. Disinclination to travel is not insured.

### (vii) Preferred Airlines and Frequent Flyer Programmes

Travellers may retain frequent flyer programme benefits. However, participation in these programmes should not influence flight selection, which would result in incremental cost to the University beyond the lowest possible airfare. Any costs associated with personal frequent flyer programmes are the responsibility of the Traveller. The TMC are not responsible for having missed points added to personal frequent flyer programmes. Frequent flyer card numbers may be stored in the individual's online traveller profile.

### (viii) Lost Baggage

The ultimate responsibility for retrieving and compensating for lost baggage lies with the airline on which the Traveller is flying. Baggage losses can be minimised by carrying valuables (laptops, jewellery, camera, phones and important documents) as hand luggage.

If baggage is lost en route please follow these procedures:

- Report the loss to the relevant airline before leaving the airport. Travellers should obtain a lost luggage report from an airline representative in the baggage claim area
- Itemise the contents of the lost baggage; (including receipts wherever possible) this should be detailed to the airline as soon as possible once realised that the baggage is missing to aid a speedy recovery
- In your claim for lost baggage you will need to include a copy of any airline tickets and baggage claim stubs;
- If the loss is through theft, the incident must be reported to the local police and a crime report reference obtained. This will enable a claim to be made for the traveller's personal possessions and any university equipment stolen / lost.

If baggage is not delivered within a reasonable amount of time at the scheduled arrival destination, emergency essentials such as toiletries and a change of clothing may be purchased, however, good judgment should be applied to the cost of such goods.

## j. Rail Travel

### (i) Making a Domestic Rail Booking

Travellers should book their rail travel using the rail booking tool. Buying a ticket through other means including on the day at the station should be avoided where possible.

### (ii) Domestic Ticket collection

Tickets can be printed at the on-site ticket printer, which is located in the University's Security Office, or at the station from a fast ticket machine. Method of collection is selected at the time of booking and cannot be changed once confirmed. If travelling on the same day as booking the tickets, please allow 30 minutes between booking and collection at the station. If printing on-site at the University, the tickets are available immediately.

### Domestic Rail – Class of Service

Travellers should normally travel standard class on University business, any exceptions to standard class require the approval of the relevant member of the Senior Management Group and on the advice of the Principal Budget Holder where this is not the same role-holder.

### (iii) Domestic Rail Cancellation Process

Cancellations should be avoided wherever possible as a refund may not always be available and the University may incur the cost. It is advisable to always check the rules at time of booking as this will indicate whether the ticket is refundable. Cancellations can be made through the online system. If cancellation is unavoidable and tickets have already been printed, Travellers must return any unused tickets within 28 days of the outbound travel date to the address below:

PO Box 23972, Edinburgh, EH2 9AF

### (iv) Exceptions

Some tickets are not available via the TMC and should be purchased at the station, for example, Oyster Cards and any travel which does not start at a mainline station, i.e. a London tube ticket only. Costs incurred for these will be reimbursed through the expense claims process.

### (v) Making a European Rail Booking

Eurostar can be booked on line via the online booking tool. For all other European rail bookings Travellers should call or email the TMC. A ticket on departure can be arranged for Eurostar travel (These can be collected at point of departure).

### (vi) European Rail – Class of Service

The TMC will always book the lowest priced logical rail ticket. Travellers should normally travel standard class on University business. Any exceptions to standard class require the approval of the relevant member of the Senior Management Group and on the advice of the Principal Budget Holder where this is not the same role-holder.

## k. Road transport

The university policy is to minimise road transport journeys preferring public transport, cycling or walking where practically possible All drivers are expected to be familiar with the current version of the Highway Code and adhere to legal requirements and recommendations.

### (i) Use of Own Vehicles

The University is committed to achieving a significant and sustained reduction in carbon emissions. Use of private cars for long distance journeys will normally be the highest carbon option; therefore, this mode of travel should only be used by exception. Staff are encouraged to use Newcastle's car club for relevant short journeys

It is recognised that use of private cars will sometimes be the most cost effective option for short journeys, especially when more than one person is travelling. Where a trip exceeds 200 miles consideration must be given to the use of public transport, or car hire, in order to reduce the cost to the University.

The University currently operates a process of self-declaration for Travellers using their own vehicles on University business. Work is in development to include all potential drivers on the university driver permit system whether using own vehicle or otherwise. Those who use their own vehicle are required to declare that they:

- Hold a valid UK driving licence
- Have appropriate business use insurance cover
- To the best of their knowledge the vehicle they intend to use is fit for purpose, has current road tax, is properly maintained, is in a roadworthy condition and where applicable has a current MOT certificate; and have not been advised that they are unable to drive on medical grounds and they are not aware of any medical condition that would make it unsafe or prevent them from driving.

Claims for mileage should provide full details of the journey including starting point, places visited and the point at which the journey ended, and total business mileage. Mileage incurred while on University business will be reimbursed at the following rates:

- Car/Van
  - First 10,000 miles per tax year — 45p per mile
  - Over 10,000 miles — 25p per mile
- Motorcycle — 24p per mile
- Bicycle — 20p per mile

The cost of toll bridges and tunnels will be reimbursed if they form part of a business journey. Parking costs incurred in the course of travelling away from home and the normal place of work may be claimed. The cost of parking at your normal place of work cannot be claimed. Long-term airport parking can be extremely expensive: Travellers should consider using alternative options such as taxis, booking in advance or the use off-site car parks to reduce costs.

### (ii) Car Rental

The use of hire cars can often be a cost effective alternative mode of transport and should be considered; particularly where more than one Traveller is travelling. The University has a car hire contract and details can be found on Northumbria University website Travel Hub/Travelling for Work/ car hire.

The university has a policy to use:

- Category B cars for sole driver usage, thereby reducing carbon emissions
- Category C cars for more than one person using the hire car.
- MPV / Mini MPV depending on number of people and amount of luggage
- Category F cars are only for prestige/executive hires

Any other type of hire vehicle would need senior management approval and be supported by good reason, e.g. health & safety grounds or amount of luggage.

The university motor insurance covers all drivers with a valid driver's permit driving a hire vehicle for university business. Any damage will result in a charge to the faculty/department up to the excess applied by the motor insurer.

Once a driver has an up to date drivers' permit, hire cars can be booked via their departments' resource administrator. Hire cars should be used in all cases where a vehicle trip exceeds 200 miles and public transport is not possible.

Additional fuel for business journeys should be purchased by the Traveller will be reimbursed on production of receipts.

### (iii) Fines & penalties

Parking fines, driving offence fines and similar charges will not be reimbursed. Road users should be aware that the maximum fines are due to increase.

### (iv) University Taxi Account

The University operates a taxi account. Each Faculty and Service is allocated a user code within this account, under the control and authority of the Principal Budget Holder. Only the following journeys are permitted:

- Early morning or late night business journeys when public transport is not easily accessible or when the cost of parking a car is more expensive
- Use of taxi journey for external guests and VIPs to and from events and activities at the University or other regional locations
- At the discretion of Principal Budget Holders to ensure staff safety, security or wellbeing

## l. Home to Work

Journeys between home and your normal place of work are regarded as private journeys and the cost of such journeys cannot be reclaimed. Car sharing is encouraged and there are options to gain discounted public transport (see staff benefits on the intranet). To find out more about car share options please contact the Sustainability Manager on extension 7068 (0191) 243 7068. Journeys away from the University on business are regarded as business journeys. Your normal place of work is the start and finish location for travel claims except where it is more economical for the claim to start at your home address, or where it is necessary to travel directly from your home address (for example, to catch an early train at a local railway station.)

### m. Accommodation Arrangements

Overnight accommodation should not ordinarily be arranged for Travellers travelling to a UK destination where the meeting/event commences after 11.00am and concludes before 5.30pm.

## 4. Accommodation Procedure

### a. Making a Hotel Reservation

Hotel reservations should be made through the online booking tool and not directly with the hotel. Reservations should be made as far in advance as possible to enable the TMC to negotiate the most favourable rate.

If a hotel reservation needs to be made / changed or cancelled out of business hours (Mon-Fri 8.45-5:30pm), this should be done through the online booking tool. In the event that this is not possible, the Traveller should contact the TMC out of hours service on 0207 8439602.

### b. Making a Group Hotel Reservation

For bookings of 10 persons or more please contact the TMC by phone on 0161 8198935 or email groups@keytravel.com

### c. Hotel Selection Guidelines

The University has a preferred hotel programme and Travellers should use this accommodation where available. If there is a need to book outside of the programme a justification (and online approval) will need to be supplied through the online booking tool system. All preferred hotels are deemed an acceptable level of comfort by the University. The accommodation available within the programme will be reviewed periodically. The TMC guarantees all hotels for late arrival.

### d. Hotel Upgrades

Travellers are entitled to stay in a double room for single occupancy, where available. Travellers may accept room upgrades if the upgrade is at no additional cost to the University.

### e. Hotel stays of longer duration

Staff staying a week or longer should make their requests as far in advance as possible which will enable the TMC to negotiate a more favourable rate.

### f. Hotel Spending Guidelines

#### (i) UK Hotel and Accommodation Costs

Hotel costs should not exceed £180 per night in London, £85 in Newcastle upon Tyne or £80 per night elsewhere in the UK. The online booking tool will not allow Travellers to make a booking that exceeds these rates until line manager approval has been given. Charges for room and breakfast will be invoiced directly (subject to hotel acceptance) to the University and this information will be displayed on the confirmation documents.

The cost of Wi-Fi and hotel parking can also be covered by the University, this will need to be paid by the traveller and claimed via the expenses process.

The cost of all business calls will be refunded when included as identifiable items on an accommodation receipt.

The cost of items of a personal nature, such as alcoholic mini bar items, newspapers or pay per view TV will not be met by the University and should be settled by the member of staff upon check out at the hotel.

If a Traveller stays with a friend or relative rather than at a hotel, they may claim up to £25 per night as an accommodation allowance. This is classed as a taxable benefit so is subject to income tax (this must be claimed via the expenses process).

### (ii) International Hotel and Accommodation Costs

International hotels should be booked through the TMC, and where possible, charges for room and breakfast will be invoiced directly to the University (subject to hotel acceptance).

In certain countries it is not always possible for the University to be invoiced directly and Travellers may have to settle their bill on departure either via corporate credit card or reclaim the costs through the expense claims process. The TMC will advise the Traveller if the University cannot be invoiced directly at the time of booking and the Traveller should verify prior to departure.

Travellers should use a hotel that is part of the University's preferred hotel programme to ensure that accommodation is in a secure and safe location and is of an acceptable standard.

The following table includes indicative rates that are acceptable to the University in the most frequently visited destinations. If these rates are exceeded approval will be required by the relevant budget holder;

| | |
|---|---|
| Colombo (Sri Lanka) | £170 per night |
| Hong Kong | £250 per night |
| Jakarta | £200 per night |
| Kuala Lumpur | £170 per night |
| Moscow | £340 per night |
| Nigeria | £200 per night |
| Penang | £170 per night |
| Seoul | £208 per night |
| Singapore | £200 per night |
| Terre Rouge | £183 per night |
| Tripoli | £236 per night |
| Other major cities outside UK | £150 per night |
| USA | £220 per night |

## g. Hotel Cancellation Procedure

The cancellation guidelines for individual hotel reservations will be displayed at the time of booking. Travellers will be requested to indicate that they have read and understood this. It is advisable not to book advance purchase rates unless the travel is almost certain, as this type of rate is non-refundable. Should a Traveller need to cancel the hotel out of business hours this should be done via the online booking tool or contact the TMC on their out of hours' number.

Travellers will be held responsible for "no-shows" as the full hotel cost will be charged to the University. The Principal Budget Holder (or their nominated signatories) will be notified of any costs charged back to their cost centre, when a Traveller has booked rooms and failed to cancel as these are chargeable.

## h. Hotel Frequent Guest Schemes

Many hotels have frequent guest schemes that reward Travellers with free accommodation in exchange for a given number of paid nights at the hotel. Travellers may retain rewards from such schemes for personal use, however, participation in these schemes will not influence the University's preferred hotel programme. Bookings should be made in line with this Policy and wherever possible the preferred hotel programme should be used. Any hotel bookings that exceed the University's approved rates (see section 7.6) will be reported via an exception report on a monthly basis to the line manager. Travellers must collect their points directly with the hotel during their stay. Loyalty card numbers may be stored within the online booking tool personal profile.

Any membership fees associated with joining these schemes are not reimbursable.

## i. Subsistence

### (i) UK Expenses

If Travellers are away from home and their normal place of work on University business in the UK they may claim for the cost of meals. This can be up to the value of £25 per day for the UK outside of London, and £35 per day for London locations. Receipts must be submitted with claim forms.

For travel within the UK, Travellers leaving home prior to 7:00am are permitted to claim for the cost of breakfast and, if arriving home after 7:00pm are permitted to claim for the cost of dinner. Receipts must be submitted with claim forms.

The UK subsistence rates for food and non-alcoholic drinks are.

- 6 hours away from home or normal place of work £7
- 12 hours away from home or normal place of work £12
- Away from home overnight £25
- Away from home overnight – London £35

Claims will only be reimbursed on the production of receipts

### (ii) International Expenses - Per Diem Rates

For travel outside of the UK, Travellers are entitled to an international per diem (daily) allowance. The per diem allowance is paid in advance and covers subsistence, personal taxi fares, telephone calls and access to the internet for personal use, if required.

The per diem rates for individual cities are available at the following website:

http://www.northumbria.ac.uk/static/5007/finpdf/perdiemrates.pdf

The per diem rate must not be exceeded for the total number of days duration of travelling on University business. Upon return, the traveller must confirm to the Payroll department that the trip

was completed and the monies incurred on University-related business. To facilitate this, Payroll will contact the Traveller within 30 days and provide the relevant form for completion and return. If this procedure is not adhered to, the University reserves the right to deduct the per diem allowance from the Traveller's salary upon 60 days of completion of the trip.

Where the Traveller does not obtain a per diem but instead obtains a pure currency advance payment, they must submit an Employee Expense Claim Form to the Payroll department to a value which exceeds the advance or should return the excess amount by following the relevant procedure as documented at:

https://www.northumbria.ac.uk/staff/travelhub/travelfor/?view=Standard

If this procedure is not adhered to, the University reserves the right to deduct the advance from the Traveller's salary upon 60 days of completion of the trip.

Relevant forms supporting these procedures can be found at:

https://intranet.northumbria.ac.uk/facultiesandservices/hri/quicklinks/azforms/

## j. Personal/Holiday Travel

The TMC serves the business travel needs of the University and therefore does not assist with personal travel (except when personal travel is in conjunction with business travel). Priority is always given to business-only travel requests. The TMC are unable to assist with personal hotel, car and flight bookings.

## k. Combining Personal Travel with Business Travel

Personal travel may be combined with business travel. The TMC will seek authorisation for such requests from the University prior to booking travel. Please also see the Insurance section 5.3.3 for information regarding insurance cover for combined business and personal travel.

## l. Use of University-Negotiated Hotel Rates for Personal Travel

The University has pre-negotiated corporate hotel rates for preferred hotels. These rates may also be used for personal travel. At the time of making personal bookings (directly with the hotel) you will need to state that you require the Northumbria University corporate rate.

## m. Conferences

The University may fund the costs of courses, conferences or trade conventions which support the objectives and priorities of the Corporate Strategy and demonstrate value for money. For those travelling to academic conferences in the UK or overseas, attendees should receive approval from their line manager, and should apply first for external funds to support attendance where these are available. The booking of Conferences cannot be done using the TMC.

For those colleagues travelling to UK conferences and educational events, it should be noted that multiple attendees at the same event should be by exception only. For approval for attendance at events and conferences a clear contribution to university objectives will need to be evident. Where colleagues are the Northumbria representative at a UK event a short report of the event should be provided to the relevant line manager.

### n. Complaints Procedure

Should Travellers experience any problems with their journey, these should be reported to the TMC so they can assist with the complaint and, where necessary, obtain refunds and compensation if applicable.

## 5. Other Expenditure

### a. Purchase of low value sundry items

Where it is not possible to use a University purchase card the University will reimburse the cost of low value items purchased by Travellers on behalf of the University, this includes purchases made via the internet and telephone.

Items below £100 should normally be reimbursed from petty cash. Except in emergency situations, the maximum claim for items purchased in the UK is £250 per claim. Each item claimed for should be supported by original receipts or suitable documentation for electronic ordering.

### b. Subscriptions

The University does not pay for personal subscriptions to professional organisations and clubs.

### c. Reimbursement for Business Telephone Calls

If Travellers are required to make business calls using their home or personal mobile telephone, they may claim the VAT inclusive call costs. Claims must be supported by the original bill.

## 6. Corporate Gifts

This section of the Expenditure Policy should be read in conjunction with the principles outlined in the University's Gifts and Hospitality Policy which can be found on the Northumbria University website.

### a. General Principles

Gifts must be reasonable and appropriate and must not exceed normal business courtesy. The primary purpose of gifts should focus on establishing cordial relationships with business partners and/or presenting the University in a favourable manner.

### b. Offering gifts

Please note all offers of gifts should be in line with the Gifts and Hospitality Policy. Cash should not be offered as a gift.

Prior to purchase the approval of the Executive Dean or Director or, in the case of members of the University Executive, the Vice-Chancellor, is required for:

- All gifts of gift cards or vouchers, irrespective of value or recipient;
- All gifts intended for a foreign public official, irrespective of value; and all gifts with a value of over £45.

In the case of members of the University Executive, all gifts offered are to be approved by the Vice-Chancellor and recorded in a Gifts & Hospitality Register kept by the University Secretary.

Any gifts offered by the University should not exceed £100 in value.

## 7. Corporate Hospitality and Business Entertainment

This section of the Policy should be read in conjunction with the principles outlined in the University's Gifts and Hospitality Policy.

Expenditure on corporate hospitality and business entertainment can take many forms. This policy covers both ***external and internal*** activities procured using corporate credit cards, expenses, purchase cards, purchase orders, or petty cash, and the use of the University's internal catering and hospitality system.

### a. General Principles

The primary purpose of hospitality should focus on establishing cordial relationships with business partners and/or presenting the University in a favourable manner.

Costs relating to the provision of hospitality will be reimbursed where it is necessary to build or to maintain effective relationships or lasting business benefits with local, national and international clients.

#### (i) Offering Hospitality

Hospitality is defined by the offering or providing reception and treatment of guests or strangers, the quality or disposition of receiving and treating guests and strangers in a warm friendly environment which may involve drinks subsistence or corporate events.

Where possible, prior to purchase the approval of the Executive Dean, Director or, in the case of members of the University Executive, the Vice-Chancellor, is required for:

- All hospitality intended for a foreign public official, irrespective of value and whether provided in the UK or abroad;
- All hospitality over the value of £45 per person.

Staff offering hospitality and entertainment should ensure that:

- The hospitality is not offered as an inducement or reward
- The list of attendees and a record of the intended benefits to the University is kept and can be provided when requested
- Appropriate prior authorisation is given by the Executive Dean, Director or member of the University Executive
- The most senior manager present should settle the bill and claim reimbursement;
- All receipts should be produced prior to reimbursement

#### (ii) Receiving Hospitality

Line managers should at all times be mindful of any potential or perceived risk resulting from the receipt of hospitality, which might compromise – or be seen to compromise - the integrity of staff and the University.

Staff receiving hospitality or entertainment should ensure that the following criteria are met:

- That the hospitality is not intended as an inducement, which should be reported to the Head of Governance;
- Hospitality over the value of £45 per person should be approved in advance by their immediate line manager, Executive Dean, Director or member of the University Executive.
- Staff should not accept hospitality from existing or potential suppliers who are involved in a tender procedure, for the duration of the tender process, to avoid allegations of improper influence.
- In situations where the position is unclear, the request should be referred to the Head of Governance prior to a final decision.

### b. Guidelines and Rates

- The ratio of staff to external guests should ideally be one to one, but it is recognised that this might not always be possible;
- The cost of including spouses of University staff are not allowable unless it is necessary that official visitors are accompanied by their spouses;
- The cost of meals (including drinks) should be subject to the following maximum levels:
    - Lunch £30 per person
    - Dinner £45 per person
    - An element of flexibility can be exercised when offering hospitality to VIP guests, if approved in advance.
- Drinks are subject to the following considerations:
    - Staff are not permitted to drink alcohol at lunchtime, modest amounts may be provided to external guests if requested.
    - Alcoholic drinks with dinner and at hospitality events are permitted in moderation, with wines selected from the lower-priced section of the menu.
    - Alcoholic drinks should not amount to more than 30% of the total bill.
- All receipts should be produced prior to reimbursement.

### c. Record Keeping

All hospitality purchased (via SAP or using credit cards etc.) should be coded to the appropriate General Ledger code(s) to show that it is "Corporate Hospitality".

All hospitality offered, received or declined, irrespective of value, must be recorded in the relevant Gifts and Hospitality Register.

## 8. Hand Held Devices

For guidance on appropriate use of mobile devices please see the IT mobile device policy (currently being developed)

## 9. Internal Trading

Internal Trading includes the provision of catering, reprographics and stationery in the University.

Any internal trading request over £5,000 must be submitted and approved by the Principal Budget Holder before committing to the activity.

## 10. Staff Meetings, Development Days, Retirement and Ad Hoc Celebrations

### a. Staff Meetings

Staff Meetings should be held on campus. The University's internal catering services should be used to provide refreshments at meetings with external guests in attendance, or at staff-only meetings scheduled over meal or break times, or where an agenda may require a whole morning or afternoon session. The use of externally-provided catering is not permitted.

### b. Staff Development Days

Staff development events should normally be held on campus and reasonable hospitality (tea, coffee, light working lunch) may be provided. The University has several catering facilities and their use is encouraged, as is the use of Boardroom 1 and 2 or Training Suite, the Great Hall all located in Sutherland Building. There should be little need for external hospitality for staff or students. Off-campus away days should only be held if there is no suitable University space.

The cost of external events will be met only if approved in advance by a member of the University Executive and supported with the business purpose and benefits, indicative costs and the names of all staff involved. Approval should take cognisance of reputational consequences, value for money and alternative internal venues available.

It is not appropriate for alcohol to be served at daytime events.

### c. Retirement, Leaving Parties and Personal Gifts

Expenditure on retirement and leaving parties should be limited to £10 per head. Claims should show the purpose of the event, internal location (external location not permitted) and the number of people attending.

Personal gifts such as leaving presents for staff or students may be funded by a collection of donations from individuals. Gifts to members of staff or students should not be made from University funds, other than in exceptional circumstances such as bereavement or serious illness (when the provision of flowers may be appropriate, and should be approved by the Principal Budget Holder).

A suitable leaving gift may be appropriate for people who have provided substantial unpaid service to the University, but this should be agreed on a case-by-case basis by a member of the University Executive or the Chair of the Board of Governors.

### d. Christmas Parties

Christmas Parties should be modest and equitable across all Faculties and Services, with a maximum contribution by the University of £15 per head for food and drink. Events should be held on University premises and all relevant staff should be invited.

### e. Other Ad Hoc Celebrations

Such events should be timely, modest and held on University premises. They should be approved in advance by the Principal Budget Holder and the University's contribution should not exceed £10 per head. All relevant staff should be invited.

## 11. Expense Claims and Payment

### a. How to claim

An employee expenses claim form should be completed for all expenses incurred that are not directly invoiced to the University with receipts supporting the claim. This claim must be approved by the relevant authorised signatory. (Claim forms can be found at

https://one.northumbria.ac.uk/hr/home/HR%20Forms/Travel%20Expenses%20for%20Employees.xls

Once authorised, the claim should be sent directly to the Payroll Section in Human Resources for payment.

Periodically, Human Resources will audit a representative sample of the expense claim forms. Any attempt to submit a false claim will be viewed as serious and may result in disciplinary action and potential legal proceedings.

Corporate Company Barclaycard users should not include Barclaycard expenditure on expense claims. Cardholders should follow the guidelines issued to them for Company Barclaycard reconciliation of expenditure.

### b. Approval of claims

Authorised signatories should review claims and ensure that:

- The journeys and/or expenses were properly and necessarily incurred on behalf of the University;
- The claim has been correctly completed and complies with this Policy;
- As far as the authoriser is aware, there has not been any previous payment against the claim from any source.
- All claims submitted are in line with the Travel Policy and all exceptions should be declared.

## 12. Administration Document History

### Revision History

**Date of this revision:**

**Date of next revision:**

| Revision date | Previous revision date | Summary of Changes | Changes marked |
|---|---|---|---|
| 09/10/2013 | n/a | First draft and format of content | |
| 10/10/2013 | n/a | Draft format for grammar and spelling | |
| 16/10/2013 | n/a | Changes to format and some content changes | |
| 05/12/2013 | n/a | Changes to format and some content changes | |
| 18/12/2013 | n/a | Changes to format and some content changes | |
| 20/12/2013 | n/a | Changes to format and some content changes | |
| 07/01/2014 | n/a | Changes made to format | |
| 05/02/2014 | n/a | Changes to format and content changes | |
| 10/03/2014 | n/a | Changes to format and content changes | |
| 14/03/2014 | n/a | Changes to format and content changes | |
| 26/03/2014 | n/a | Changes to format and content changes | |
| 08/04/2014 | n/a | Changes to format and content changes | |
| 16/04/2014 | n/a | Changes to format and content changes | |
| 24/04/2014 | n/a | Changes to format | |
| 19/05/2014 | n/a | Approved by Employment and Finance Committee | |
| 21/05/2015 | n/a | Proof read | |
| 29/06/2016 | n/a | Track changes proposed | |
| 05/07/2016 | n/a | Approved by University Executive | |
| 26/07/2016 | n/a | Track changes agreed | |

## Approvals

This document has gone through the following approvals.

| Name | Title |
|---|---|
| Chris Reilly | Chief Operating Officer |
| Andrew Jefferson | Interim Finance Director |
| TBC | Pro Vice Chancellor (International Development) |
| Rob Carthy | Director of International Development |
| University Executives | n/a |
| Employment and Finance Committee | n/a |

## Distribution

The document should be distributed to:

| Name | Title | Date of Issue | Version | Reason |
|---|---|---|---|---|
| Key Travel Limited | n/a | 01/09/2015 | V25 | Notification to all Travellers |
| Vice Chancellor's Office | n/a | 27/05/2014 | V25 | Notification to all Travellers |
| International Office | n/a | 27/05/2014 | V25 | Notification to all Travellers |
| Faculty Business Managers | n/a | 27/05/2014 | V25 | Notification to all Travellers |
| Faculty Resource Managers | n/a | 27/05/2014 | V25 | Notification to all Travellers |
| University PA's | n/a | 27/05/2014 | V25 | Notification to all Travellers |
| University travellers | n/a | 26/07/2016 | V26 | Notification to Travellers |

**EXHIBIT D**

**STANDARD MODEL CLAUSES FOR THE TRANSFER OF DATA OUT OF THE EEA**

**Schedule 1**

**Exhibit D**

**DATED**

---

# STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

## UNIVERSITY OF NORTHUMBRIA AT NEWCASTLE

## AND

## CIVITAS LEARNING INC.

## CONTENTS

### CLAUSE



### ANNEX

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

| | |
|---|---|
| Name of the data exporting organisation: | University of Northumbria at Newcastle, Sutherland Building, College Street, Newcastle upon Tyne, NE12 9JN |
| address: | ..... |
| tel: | 0191 2274686..... |
| fax: | ..... |
| e-mail: | |
| Other information needed to identify the organisation | ..... |
| **(the data exporter)** | |
| Name of the data importing organisation: | Civitas Learning Inc. 100 Congress, Austin, Texas, 78701, United States of America |
| address: | ..... |
| tel: | 001 512 6927175 |
| fax: | ..... |
| e-mail: | ..... |
| Other information needed to identify the organisation | ..... |
| **(the data importer)** | |

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex A.

## 1. DEFINITIONS

For the purposes of the Clauses:

(a) **personal data, special categories of data, process/processing, controller, processor, data subject** and **supervisory authority** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) **the data exporter** means the controller who transfers the personal data;

(c) **the data importer** means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its instructions and the terms of

the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) **the sub-processor** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract;

(e) **the applicable data protection law** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) **technical and organisational security measures** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## 2. DETAILS OF THE TRANSFER

The details of the transfer and in particular the special categories of personal data where applicable are specified in Annex A which forms an integral part of the Clauses.

## 3. THIRD-PARTY BENEFICIARY CLAUSE

3.1 The data subject can enforce against the data exporter this clause 3, clause 4(b) to clause 4(i), clause 5(a) to clause 5(e) and clause 5(g) to clause 5(j), clause 6.1 and clause 6.2, clause 7, clause 8.2 and clause 9 to clause 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this clause 3.2, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the sub-processor this clause 3.3, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2, and clause 9 to clause 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

## 4. OBLIGATIONS OF THE DATA EXPORTER

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Annex B to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to clause 5(b) and clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Annex B and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and

(j) that it will ensure compliance with clause 4(a) to clause 4(i).

## 5. OBLIGATIONS OF THE DATA IMPORTER

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Annex B before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex B which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with clause 11; and

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

## 6. LIABILITY

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in clause 3 or in clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data

importer or its sub-processor of any of their obligations referred to in clause 3 or in clause 11 because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in clause 3 or in clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

## 7. MEDIATION AND JURISDICTION

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

## 8. COOPERATION WITH SUPERVISORY AUTHORITIES

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5(b).

## 9. GOVERNING LAW

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely England, United Kingdom.

## 10. VARIATION OF THE CONTRACT

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

## 11. SUB-PROCESSING

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely England, United Kingdom

11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

**12. OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES**

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter
(**University of Northumbria at Newcastle**):

Name (written out in full): Section 40
Position:

Address:
Other information necessary in order for the contract to be binding (if any):

Signature

On behalf of the data importer
(**Civitas Learning Inc**):

Name (written out in full): Section 40
Position:
Address:

Signature

## Annex A.

to the Standard Contractual Clauses
This Annex forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Annex A.

| | |
|---|---|
| **Data exporter** | |
| The data exporter is (please specify briefly your activities relevant to the transfer): | A Higher Education Institution and an exempt charity |
| **Data importer** | |
| The data importer is (please specify briefly your activities relevant to the transfer): | Civitas Learning Inc provides a predictive analytics platform that helps higher education institutions to build a strategic analytics infrastructure |
| **Data subjects** | |
| The personal data transferred concern the following categories of data subjects (please specify) | Students of the data exporter |
| **Categories of data** | |
| The personal data transferred concern the following categories of data (please specify) | Anonymised SITS and Blackboard data (phase 1)<br>Live data from the pilot population (phase 2) |
| Special categories of data (if appropriate) | |
| The personal data transferred concern the following special categories of data (please specify) | N/A |
| **Processing operations** | |
| The personal data transferred will be subject to the following basic processing activities (please specify) | Historical data will only be transferred to the data importer for the purposes of testing new functionality and feature testing. |
| **DATA EXPORTER (University of Northumbria at Newcastle)** | **DATA IMPORTER (Civitas Learning Inc.)** |

Section 40

[redacted]

## Annex B.

to the Standard Contractual Clauses
This Annex B forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with clause 4(d) and clause 5(c) (or documents/legislation attached):

- CivitasLearning Information Security Policy;
- CivitasLearning Handling Partner Data;
- CivitasLearning Incident Response plan;
- CivitasLearning Disaster Recovery plan;

.....
.....

**Liability**

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.

# Civitas Learning - Information Security Policies

Section 40 [redacted]

**February 23, 2016**
**Version 3.0**

## Table of Contents

## Introduction

The rules and requirements set forth in this document apply to all employees, interns, contractors, and sub-contractors of Civitas Learning. Prior to being provided access to any assets belonging to or in the care of Civitas Learning, this documentation must be read, reviewed, and formally acknowledged by the individual acting in any of the aforementioned roles.

## Purpose

This document seeks to provide overviews of the nature of data and information systems that Civitas Learning manages, to explicitly state the principles surrounding data protection that all Civitas Learning staff must agree with and adhere to, and exhort all employees to be proactive in their pursuit of data protection, security, and compliance.

## Definition of Terms and External References

Any language which is denoted in *italicized* text will be formally defined within the Civitas Learning Glossary of Terms document. That file along with any other external documentation which supplements this policy may be found at the following Box.com URL:

Section 43 [redacted]


## A - Information Security and Risk Management

1. **Information Security Policies**
    a. The Civitas Learning – Information Security Policies (this document) and all supporting documentation referenced within this file must be reviewed at least annually and updated as needed to reflect changes to business objectives, technology enhancements, and risk factors to the company.
    b. The Civitas Learning – Information Security Policies (this document) must be approved by the Director of Security & Compliance or the individual within the company that is otherwise formally assigned the duties of a Chief Security Officer.
    c. All personnel must acknowledge upon hire and with each updated release of the documentation that they have read the Civitas Learning – Information Security Policies and accept responsibilities for adhering to the requirements.
2. **Security as a "business-as-usual" approach**
    a. An internal group of subject matter experts (the Security Council), chaired by the Director of Security & Compliance will provide guidance and input related to security on all project management efforts.
3. **Risk Assessment**
    a. A formal, documented risk assessment must be performed at least annually and should be performed after moderate to significant changes to the company environment.
    b. The assessment should identify company assets.
    c. The assessment should identify potential threats along with their likelihood and impact.
4. **Business Organization**
    a. The company must maintain an organizational chart of company personnel.
    b. The company must define job titles.
    c. The company must define responsibilities associated with each position.
    d. The company must review job titles and responsibilities annually and update as necessary to ensure that job roles and duties are accurate and up to date.
5. **Security Awareness Program**
    a. Employees must undergo security best practices training upon hire and at least annually thereafter.
6. **Acceptable Use Policy**
    a. Personnel must acknowledge the company's Acceptable Use Policy.
    b. Personnel must acknowledge upon hire and with each updated release of the documentation that they have read the policies and accept the responsibilities of adhering to the requirements.
7. **Non-Disclosure**
    a. Personnel must acknowledge the protection of information proprietary to the company.
    b. The non-disclosure/confidentiality agreement must be reviewed annually and updated to the reflect the current needs of the business.
8. **Employee Background Checks**
    a. Background checks must be performed on personnel prior to employment.
9. **Third Party Relationships**
    a. Vendors
        i. A list of vendors used to support product development, delivery and maintenance must be maintained

ii. The list of vendors must be reviewed annually and kept up to date to reflect the current environment.

b. The company must monitor, review, and audit vendor service level to ensure it is within the expectation of company policies and contractual agreements.

**10. Compliance to the Civitas Learning – Information Security Policy**

a. Must
   i. Security controls and guidelines which are identified as "must" are required to be implemented in order to be in compliance with the Civitas Learning – Information Security Policy.
   ii. Solutions and strategies which operate as part of the Civitas Learning environment and do not meet these requirements are to be remediated as quickly as possible in a manner that is responsible to business continuity.

b. Should
   i. Security controls and guidelines which are identified as "should" are recommended solutions, but are not required for compliance to the Civitas Learning – Information Security Policy.

c. Exceptions
   i. Solutions and strategies which operate as part of the Civitas Learning environment and are unable to meet the requirements or recommendations outlined with the Civitas Learning – Information Security Policy (this document) must formally request an exception.
      1. The exception must be formally documented.
      2. The exception must be formally evaluated for risk
      3. The documented risk must be accepted by the Security Council and approved by the Director of Security & Compliance or the individual within the company that is otherwise formally assigned the duties of a Chief Security Officer.


## B - Data Classification and Protection

1. **Classification of Data**
    a. **Personally Identifiable Information (PII)**
        i. Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (NIST Special Publication 800-122)
    b. **Proprietary Information and Intellectual Property (IP)**
        i. Non-public information rightfully obtained, developed, or produced by or for the benefit of Civitas Learning and its employees. Proprietary information and Intellectual Property is owned by Civitas Learning, not the employee. Employees will provide Proprietary Information or Intellectual Property to non-Civitas Learning personnel only when properly authorized by Civitas Learning executive staff. A non-disclosure agreement will be in place with the recipient prior to the release of any Proprietary Information or Intellectual Property.
        ii. Proprietary information and Intellectual Property must be protected through processes which ensure the data is not exposed to any unauthorized party, internal or external to Civitas Learning.
    c. Public Information
        i. Public information is information which has been circulated outside the company through the direction and oversight of the Civitas Learning executive staff and is openly available and accessible to the public.
2. **Retention of PII Data**
    a. Storage of PII should be kept to the minimum required for legal, regulatory, and/or business purposes.
    b. As soon as data is no longer required for legal, regulatory, and/or business purposes it should be disposed of according to company policy (this document).
    c. Every quarter, an effort should be conducted for identifying and deleting stored data that exceeds an agreed upon retention period or is no longer required for legal, regulatory, and/or business purpose.
3. **Restriction of PII Data**
    a. Employees must not handle PII unless explicitly authorized to do so for a business purpose.
    b. PII must not be communicated via electronic mail (e-mail), messaging technology, or any other application (internal or external) unless explicitly authorized to do so by the Director of Security & Compliance or the individual formally assigned the duties of a Chief Security Officer.
    c. PII must not be stored on local systems (laptop, desktop, or any portable devices such as a smartphone, USB drive, or tablet)
    d. PII in hard copy must be stored securely in locked cabinets, drawers, or other encasement.
4. **Protection of PII Data**

a. At Rest
    i. PII data should be destroyed wherever possible.
    ii. If unable to be destroyed, PII data should be de-identified.
    iii. If unable to be de-identified, PII data must be secured using strong encryption.
b. In Transit
    i. PII data must be secured using strong encryption, either in payload or by encapsulation, while in transit across open, public networks (802.1x style wireless or the Internet).

**5. Encryption of PII Data**

a. At Rest
    i. PII must be secured using strong encryption while at rest in a digital format.
    ii. Disk level encryption must be used as a minimum level of data protection.
    iii. File-level and Column-level encryption should be used as the preferred method of data at rest protection.
    iv. Key Management
        1. Encryption keys should be secured while at rest.
            a. Key may be secured using a key-encrypting key (KEK) that is stored separately from the data-encrypting key (DEK).
            b. Key may be secured using a secure cryptographic device.
            c. Key may be secured as part of a key component or key share.
            d. Key must not be secured in an unencrypted format as part of application code.
        2. Keys must be made available to the minimum number of personnel.
        3. Keys must be communicated between parties using a secure communication channel (i.e. encrypted channel).
        4. DEKs and KEKs managed by Civitas Learning must be rotated at least every 3 years. Encryption keys securing data on behalf of Civitas Learning and managed by third parties should be rotated at least every 3 years.
        5. Keys must be replaced immediately if the integrity of the key has been compromised.
b. In Transit
    i. Strong cryptography and/or security protocols (IPSEC or TLS 1.2 or greater as of this writing) must be employed

**6. Disposal of PII Data**

a. Hard Copy
    i. PII in a hard copy format must be disposed of through a cross-cut shredder or other method of destruction such that the information is unable to be read or reconstructed.
    ii. If the hard copy is not immediately destroyed, it should be held in a locked or otherwise secured container until proper destruction takes place.
b. Digital Format
    i. Where possible, PII should be disposed of using a secure wipe process.
    ii. If a secure wipe process is not possible, PII data should be expunged in such a manner that it is unable to be retrieved and made readable.

iii. If data is unable to be expunged sufficiently, the physical media must be destroyed in such a manner that data is impossible to retrieve from the remains.

## C - User Management and Access Control

1. **Access Rights and Privileges**
    a. Grant access to systems and information on a need-to-know basis
    b. Account rights must be assigned on the premise of least-privileges required to perform job role.
2. **Accounts and Authentication**
    a. All accounts must use a unique login to access applications, systems, networking components, and data.
        i. Any exception to this requirement must be proposed by the process owner and approved by the Security Council.
    b. All accounts must use at least single-factor authentication credentials to access an application, system, networking component, or data.
    c. All remote network access by a roaming user must use 2-factor authentication.
    d. Shared accounts should not be used for any administrative function.
        i. A formal exception process which incorporates dual control must be enforced in scenarios where a shared account is used.
    e. Shared credentials should not be used for any administrative function.
        i. A formal exception process which incorporates dual control must be enforced in scenarios where shared credentials are used.
    f. Implement a technical control which logs a user out of a session after no more than fifteen (15) minutes of inactivity.
3. **Access Review and Validation of Privilege**
    a. Review user accounts, access rights, and privileges at least every 30 days. Remove or disable accounts which are no longer used or required for business.
    b. Immediately revoke access for terminated users.
4. **Passwords, Passphrases, and Authentication Credentials**
    a. All credentials must be secured using strong encryption when stored at rest and in transit
    b. All passwords and passphrases must [redacted]
    c. All passwords and passphrases must contain alpha characters, numeric characters, and special characters
    d. All passwords and passphrases must be changed [redacted]
    e. A user's password or passphrase may not be the same as any of the individual's previous [redacted]
    f. A user ID must be locked out after no more than [redacted] attempts. The account should remain locked for [redacted] until a system administrator re-enables the account.
    g. Upon change of a user's password or passphrase, the new credential must be unique and must be changed again after the first use.

## D - Securing Networks and Systems

1. **Maintain current diagrams representative of the business environment**
    a. **Network Diagram**
        i. At least one or more logical network diagrams which include all segments and resources.
        ii. The diagrams must include wired networks, wireless networks, and virtual networks.
        iii. The diagrams must be reviewed annually and updated to reflect the most current environment.
    b. **Data Flow Diagram**
        i. At least one or more logical flow charts which document how data is acquired, processed, stored, and disposed of.
        ii. The diagrams must be reviewed annually and updated to reflect the most current environment.
2. **Define Configuration Standards for all systems, applications, and networking components.**
    a. Change vendor supplied defaults
    b. Disable unnecessary accounts
    c. Disable unnecessary services
3. **Remote, non-console access must be secured using strong encryption.**
4. **Maintain an inventory of systems.**
    a. List should include a unique identifier for each entry.
    b. List should include a custodian for each entry.
    c. List should include relevant technology details. At a minimum:
        i. Vendor
        ii. Version
5. **Patches and Updates.**
    a. External sources should be used to stay aware of latest threats and related patches, updates, and workarounds to address mitigation and remediation.
    b. Security patches and updates determined to be critical must be applied within Section 43 All other patches and updates should be applied within Section 43
6. **Firewalls and Network Access Control**
    a. Network access control which limits traffic must be placed between any Civitas Learning resource and any third party network, e.g. the Internet, a Partner, a Vendor.
    b. A stateful packet inspection firewall or other stateful mechanism should be used for network access control.
    c. A web application firewall (WAF) should be deployed for public-facing (Internet) resources.
    d. Inbound and outbound traffic must be limited to only that which is necessary for business purposes. All other traffic must be denied, dropped, or rejected.
    e. Ports and Services
        i. Specific ports and services must be defined within access control lists and rule-sets.
        ii. All ports and services which are authorized must be documented
            1. Documentation should include the application or service associated

with the port.

f. Direct access to Civitas Learning resources from the Internet is prohibited.

7. **Wireless Networking**
   a. WPA2 is the minimum security protocol level required to secure any wireless network.
   b. Pre-shared keys used to authenticate access to a non-guest wireless network must be Section 43
   c. Pre-shared keys used to authenticate access to a non-guess wireless network must be changed immediately following the departure of any employee, contractor, intern, or subcontractor from the company.
   d. Visitors and all other individuals that have not been given explicit authorization to use the corporate wireless network must use a "guest" network.
      i. The "guest" network must not have direct network connectivity to the corporate wireless network.
8. **Laptop computing**
   a. Disk-level encryption must be deployed for all laptop computing devices.
9. **Mobile Handheld Computing Devices**
   a. A numeric PIN or complex swipe pattern must be used for authentication to portable, handheld computing devices (smart phones and tablets) that are used to access any form of business information.
   b. Portable, handheld computing devices (smart phones and tablets) must be available for remote wiping capabilities by the Civitas Learning Information Technology (IT) group with proper cause.
10. **Bring Your Own Device (BYOD)**
    a. Personally owned devices are prohibited for business use. Exceptions must receive management approval and register with the IT group.
    b. Personally owned devices must not connect to any Civitas Learning network, wired or wireless, with the exception of appointed "guest" networks.

## E - Secure Coding and Development

1. Training and Education
    a. Developers should undergo secure coding training at least annually.
    b. Developers must familiarize themselves with the top ten coding vulnerabilities as published by the Open Web Application Security Project (OWASP)
        i. http://www.owasp.org/
        ii. While OWASP specifically references web applications, the secure code principles should be applied to non-web applications as well.
2. Code Review/Peer Review
    a. Code changes must be reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices.
    b. Code reviews ensure that code is developed according to secure coding guidelines.
    c. Code reviews result in formal recommendations which are implemented prior to code release.
    d. Code review results are reviewed and approved prior to release.
3. Development/Test environments
    a. Systems, Networks, Applications, and Data used within development and testing environments must be separate from production environments with access control in place to enforce separation.
4. Separation of duties
    a. Personnel assigned duties and responsibilities within the development environment should not have access to production.
    b. A process that incorporates dual control must be implemented if an individual with responsibilities within the development environment requires access to production.
5. Production data used in development
    a. PII should not be used in development environments.

## F - Maintaining Secure Environments

1. **Technologies and Services**
    a. Onboarding
        i. Any new technology, service, or strategy must be submitted for a security review by the Security Council.
        ii. The Security Council must review the new proposal for issues which may pose threats to the company security or compliance postures.
        iii. The Security Council must approve the proposal, deny the proposal, or respond with a recommended course of action to remediate the proposal such that it can be approved.
    b. Existing
        i. A list of approved technologies (software, hardware, vendors, business process, or service) must be maintained and reviewed annually to ensure it is current and up to date.
2. **Change Control**
    a. A record must be created for each configuration or other change to a production resource
        i. Must include management authorization
        ii. Must identify owner of the deployment
        iii. Documentation of change objective
        iv. Documentation of potential change impact
        v. Must include acknowledgment of testing prior to deployment
        vi. Must include back-out procedures
    b. Changes should first be tested and evaluated for potential negative impact within a "test" or non-production network prior to deployment.
    c. Changes to any production resource should be scheduled for an acceptable, off-peak time.
3. **Test/Development Environments**
    a. Systems, Networks, Applications, and Data used within development and testing environments must be separate from production environments with access control in place to enforce separation.

## G - Monitoring Security and Potential Threats

1. **Vulnerability Management program**
    a. Vulnerability scanning
        i. A formal effort should be conducted monthly and must be conducted at least quarterly to scan for vulnerabilities to applications, systems, and networking components.
        ii. The scope of the effort should include resources that reside on all wired networks, wireless networks, and virtual networks. Exceptions to this list are test networks and development networks.
        iii. The scope of the effort should include tests against systems, applications, and networking components.
        iv. The effort should result in a formal report documenting findings, risk levels, and remediation recommendations.
        v. Findings from the effort must be reviewed and prioritized for remediation by the Security Council and approved by the Director of Security & Compliance or the individual within the company that is otherwise formally assigned the duties of a Chief Security Officer.
    b. Penetration testing
        i. A formal penetration test must be performed at least annually
        ii. The scope of the effort should include resources that reside on all wired networks, wireless networks, and virtual networks. Exceptions to this list are test networks and development networks.
        iii. The scope of the effort should include tests against systems, applications, networking components and personnel.
        iv. The effort should result in a formal report documenting findings, risk levels, and remediation recommendations.
        v. The effort should be conducted by a third party with adequate expertise and experience to perform such testing.
        vi. Findings from the effort must be reviewed and prioritized for remediation by the Security Council and approved by the Director of Security & Compliance or the individual within the company that is otherwise formally assigned the duties of a Chief Security Officer.
2. **Wireless Network monitoring (Rogue WAP detection)**
    a. A process must be conducted on at least a quarterly basis to identify unauthorized wireless access points and unauthorized devices connected to authorized wireless access points.
    b. Findings must be addressed within seven (7) days of identification.
3. **Intrusion Detection**
    a. Intrusion detection (IDS) and/or intrusion prevention (IPS) mechanisms must monitor traffic at every ingress/egress point of the network.
    b. IDS/IPS resources must automatically generate alerts when atypical or unauthorized traffic is identified.
4. **File Integrity Monitoring (FIM)**
    a. File integrity or change monitoring software must be deployed on server-class systems.
    b. The process must run at least weekly.

c. The process must monitor configuration files, boot files, and other files identified as critical for business.
d. FIM or change monitoring software must automatically generate alerts when atypical or unauthorized activity is identified.

5. **Anti-Virus (AV)/Anti-Malware/Host Intrusion Detection Software (HIDS)**
   a. Anti-virus software used to detect and prevent viruses, malware, and other malicious software must be deployed on systems running any version of the Microsoft Windows family of Operating Systems (OS).
   b. Anti-virus software used to detect and prevent viruses, malware, and other malicious software should be deployed on systems running any other OS within the company.
   c. Anti-virus software must be configured to automatically perform scans at least weekly.
   d. Anti-virus software configured to automatically update signatures at least weekly.
6. **Incident Response, Disaster Recovery, and Business Continuity Processes**
   a. Must be tested, reviewed, and updated annually.
   b. Must document specific actions, notifications, and procedures to take in the event of an incident.
   c. Must include business continuity planning and actionable procedures.
   d. Must assign responsibility of actions and procedures to specific groups or individuals
7. **Logging and Alerting**
   a. Enable logging mechanisms which capture, at a minimum:
      i. User activities
      ii. Exceptions
      iii. Faults
      iv. Information Security Events
   b. Administrator and System Operator actions must be logged.
   c. Logs and audit trails should be offloaded to a centralized repository in real-time.
   d. Log files and audit trails must be protected from unauthorized access and/or tampering.
   e. Time must be synchronized and accurate for all logging mechanisms.
      i. Clocks should be synchronized to a single, central source.
   f. All logs and audit trails must be reviewed at least weekly. Security focused logs should be reviewed daily.
      i. Any exceptions or anomalies identified must be investigated by the appropriate personnel.
   g. All logs and audit trails must be held or archived fo[redacted] Section 43

## H - Physical Security

1. **Entry controls must be employed to limit access to company offices and locations hosting technology resources and allows only those individuals who are authorized.**

## Appendix – History of Document Review

| Date | Version | Summary | Reviewers | Approver |
|---|---|---|---|---|
| **February 23, 2016** | **3.0** | **Initial publication** | Section 43 | Section 43 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Civitas Learning – Handling Partner Data

Section 40 [redacted]

**February 23, 2016**

**Version 1.0**

## Table of Contents

## Introduction

The guidelines set forth in this document apply to all employees, interns, contractors, and sub-contractors of Civitas Learning. Prior to being provided access to any assets belonging to or in the care of Civitas Learning, this documentation must be read, reviewed, and formally acknowledged by the individual acting in any of the aforementioned roles.

## Purpose

This document seeks to provide overviews of the nature of data and information systems that Civitas Learning manages, to explicitly state the principles surrounding data protection that all Civitas Learning staff must agree with and adhere to, and exhort all employees to be proactive in their pursuit of data protection, security, and compliance.

## Definition of Terms and External References

Any language which is denoted in *italicized* text will be formally defined within the Civitas Learning Glossary of Terms document. That file along with any other external documentation which supplements this policy may be found at the following Box.com URL:

Section 43 [redacted]

## Guidelines for Staff

Partner Data is defined as any information provided by an institution, which identifies attributes of faculty, staff, or student body. This data can be in the form of a direct identifier, such as an individual's name, e-mail address, or biometric record, as well as in the form of an indirect identifier, such as gender, geographic indicator, or educational marks.

In all cases, care must be taken in handling partner data. At a minimum this information must be considered proprietary to the institution and secured as personally identifiable information (PII) under the guidance and requirements of the Civitas Learning – Information Security Policy.

## Compliance & Privacy

Partner Data falls under the protection of U.S. federal[1] and international[2] laws as well as state-by-state U.S. domestic legislation where applicable. Civitas Learning must protect the privacy of all Partner Data. If any Civitas Learning staff member becomes aware of any Partner Data, the individual must maintain this information as strictly confidential.

Civitas Learning must adhere to processes that maintain compliance and privacy. These include but are not limited to:

- Use and disclosure of Partner Data is not permitted outside of its intended use as part of Civitas Learning's suite of applications.
- Partner Data should not be held for longer than is necessary or agreed to through contractual agreement.
- Partner Data should be safeguarded according to the rules and guidelines addressing PII within the Civitas Learning – Information Security Policy.
- Partner Data should not be transferred to a country or territory outside of the country or territory of origin.

[1] Family Educational Rights and Privacy Act http://www2.ed.gov/policy/gen/guid/fpco/ferpa/
[2] Data Protection Act 1998 - http://www.legislation.gov.uk/ukpga/1998/29/contents/

## Appendix – History of Document Review

| Date | Version | Summary | Reviewers | Approver |
|---|---|---|---|---|
| **February 23, 2016** | **1.0** | **Initial publication** | | Section 40 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Civitas Learning – Incident Response Plan Overview

Section 40 [redacted]

**March 10, 2017**
**Version 2017.01**

## Table of Contents

## Audience

**The guidelines and requirements set forth in this document apply to all employees, interns, contractors, and sub-contractors of Civitas Learning.**

## Purpose

**This document provides an overview of the Civitas Learning – Incident Response Plan. The document should be considered private and confidential but is available without the need of a non-disclosure agreement. Please do not re-distribute.**

## Introduction

The Civitas Learning – Incident Response Plan serves as the company's guide and process for planning and preparing for the unexpected misuse of company assets.

## Plan Overview

The Civitas Learning – Incident Response Plan documents resources and procedures to be executed in the event that an interruption of service occurs. Each support application or platform is identified containing prescriptive recovery steps. Each section also identifies departments and key personnel necessary to perform the recovery tasks and a communication chain for internal and external information updates.

The plan is reviewed every 6 months and tested annually with a simulated walkthrough including key personnel. Due to the very sensitive nature of the information and contact details contained in the plan, the document must be treated as confidential and never shared with third parties.

The Civitas Learning approach to disaster recovery is based upon the SANS Institute's Incident Handler's Handbook.[1]

## Plan Approval

The Civitas Learning – Incident Response Plan has been reviewed and approved the Civitas learning executive team and has their full commitment.

[1] https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

## Plan Phases

### Preparation

Civitas Learning does not maintain a dedicated incident response team (IRT). Rather, management of the incident response program is assigned to the Director of Security & Compliance. In the event of any malicious activity being identified, this individual will gather a team of personnel to serve as the IRT through the phases of the incident response plan

A full contact list of all individuals designated as being eligible to participate as part of an IRT is held in the Pingboard application, available through Civitas Learning cloud resources. Additional contact information for vendors is maintained by Civitas Learning IT. This list is reviewed annually for updates.

Civitas Learning maintains a repository dedicated to storing playback information documented during an investigation. This will be used for lessons learned and clarity for defining incident timeline.

Civitas Learning has developed a Crisis Communication Plan to effectively relay news of the incident and updates to stakeholders and impacted customers.

### Identification

Upon notification of a possible incident, the Director of Security & Compliance will contact the IT Manager and the DevOps Manager to begin an initial investigation. After determining scope and relevant technologies, the managers will identify resources necessary to form the IRT. These individuals will be contacted and the group will meet either at the central office as a command center or virtually depending upon time of day and availability.

Documentation responsibilities will be assigned to an individual within the IRT. All actions will be captured to notes.

Customers affected by the incident will be notified and provided with status updates every 4-6 hours.

### Containment

After isolating the incident, steps will be taken to create a short-term containment of the issue. The IRT will attempt to complete these steps but will reach out to vendors for additional insight into managed environments such Section 43 The affected resources will be backed-up to allow for offline forensic investigation.

### Eradication

All affected instances will be destroyed Section 43 New instances will be created and application stacks deployed. No data will be restored from backup to ensure that the cause of the incident will not be reintroduced to the environment. If necessary, enterprise applications for predictive analytics will have data retrained using the most current information available to provide restored service.

## Recovery

As systems and application stacks are brought back into production, the Data Quality Assurance group within Civitas Learning will be leveraged to monitor the affected environment assess current working condition. At this time, the Director of Security & Compliance will reach out to our partnering vendor to perform a penetration test on the environment if necessary to determine the efficacy of updated controls or process to deter future vulnerabilities.

## Lessons Learned

The Director of Security & Compliance will coordinate a follow-up meeting including all members of the IRT that addressed the specific incident. All documentation captured during the incident will be reviewed and updated to include any detail not recorded during the event. The documentation will live within the Civitas Learning internal wiki as a resource for annual training and refinement of the process. A general summary will be provided to management for review and formal response to follows-up and questions.

## Appendix – History of Document Review

| Date | Version | Summary | Reviewers | Approver |
|---|---|---|---|---|
| **March 10, 2017** | **2017.01** | **Update to reflect current Incident Response Plan** | Section 40 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Civitas Learning – Disaster Recovery & Business Continuity Overview

Section 40 [redacted]

**July 19, 2016**

**Version 2016.01**

## Table of Contents

## Audience

**The guidelines and requirements set forth in this document apply to all employees, interns, contractors, and sub-contractors of Civitas Learning.**

## Purpose

**This document provides an overview of the Civitas Learning – Disaster Recovery Plan. The document should be considered private and confidential but is available without the need of a non-disclosure agreement. Please do not re-distribute.**

## Introduction

The Civitas Learning – Disaster Recovery Plan serves as the company's guide and process for recovery and restoration of technology systems and services in the event that a disaster event partially or wholly interrupts business operations.

## Plan Overview

The Civitas Learning – Disaster Recovery Plan documents resources and procedures to be executed in the event that an interruption of service occurs. Each support application or platform is identified containing prescriptive recovery steps. Each section also identifies departments and key personnel necessary to perform the recovery tasks and a communication chain for internal and external information updates.

The plan is reviewed every 6 months and tested annually with a simulated walkthrough including key personnel. Due to the very sensitive nature of the information and contact details contained in the plan, the document must be treated as confidential and never shared with third parties.

The Civitas Learning approach to disaster recovery is based upon the SANS Institute's Disaster Recovery Plan Strategies and Processes.[1]

## Plan Approval

The Civitas Learning – Disaster Recovery Plan has been reviewed and approved the Civitas learning executive team and has their full commitment.

## Disaster Identification & Authorized Personnel

The following members of the Civitas Learning are authorized to declare a disaster scenario and/or the resumption of normal operations:

- Chief Executive Officer
- Chief Technology Officer
- Director of Security & Compliance

In addition, a number of internal and external disaster identifications made by technology personnel may trigger the initiation of the disaster recovery plan. External threats can be varied (environmental, denial of service attacks, cloud provider outages, etc.).

## Disaster Recovery Lead Responsibilities

Depending upon the nature of the issues presented, different team members may be appropriate for

[1] https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564

disaster response. The Director of Security & Compliance is designated as the disaster recovery lead (DRL) and will identify the necessary technical resources for a given incident and assemble a disaster response team (DRT).

DRL responsibilities:

- Determines nature and scope of the incident.
- Contacts qualified technical specialists for advice as needed.
- Identifies and assembles qualified technology specialists for the DRT.
- Escalates issues to executive management as appropriate
- Monitors progress of recovery process.
- Ensures evidence gathering, documentation, chain of custody and corrective action.
- Coordinates communication to affected Partners and third parties.

## Key Third Party Vendor Systems

Civitas Learning maintains a list of vendors that provide key services to our business strategy. The list is reviewed quarterly and updated with detailed information, including:

- Internal owners and contact information
- Vendor contact information and escalation paths.
- Contract overview and service level agreement metrics.
- Criticality level of service (Critical/Internal Delivery/Ancillary)

## Command Centers

In the event that a disaster is declared, the DRT should convene within a designated Command Center. A dedicated conference room within the corporate headquarters of Civitas Learning is the preferred Command Center. In the event that the office is unavailable due to destruction or environmental factors, two backup Command Centers are identified within the Civitas Learning – Disaster Recovery Plan.

## Disaster Plan Execution Phases

The disaster recovery plan is composed of four phases of execution:

1. Impact Assessment
    a. The DRL declares disaster state.
    b. DRT will be identified. Incident Response Team (IRT) will be identified if necessary.
    c. DRT will assemble in an agreed upon Command Center.
    d. Scope of impact will be determined.
2. Response
    a. Execution of documented response checklist for appropriate disaster symptoms.
    b. If none of the existing response checklists are deemed appropriate or adequate, the DRT (and IRT) will collaborate to determine the correct course of action.
    c. Appropriate communication to Partners, vendors, staff, and authorities (if required by

law).

3. Resolution and Recovery
    a. Agreed upon return to business as usual service levels.
4. Post-mortem
    a. DRT reconvenes to document lessons learned, improvements, and updates to plan/checklists.

## Disaster Response Checklists

Civitas Learning has established a list of disaster scenarios with procedural checklists to assist the DRT for appropriate and organized response. The lists are reviewed twice per year and relevant personnel to the technology involved walk through the respective checklist annually. Scenarios include:

- Cloud facilities inoperable.
- Cloud facilities unusable for more than 12 hours.
- Cloud facilities unusable for more than 24 hours.
- Cloud file storage destroyed.
- Tokenization facilities unavailable.
- Encryption facilities unavailable.
- Prolonged DNS outage (greater than 12 hours).
- Production applications down or unusable for more than 12 hours.
- Primary office unavailable or destroyed.

## Appendix – History of Document Review

| Date | Version | Summary | Reviewers | Approver |
|---|---|---|---|---|
| **July 19, 2016** | **2016.01** | **Update to reflect current Disaster Recovery Plan annual review.** | Section 40 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |