IMPERO SERVICES AGREEMENT

This Impero Services Agreement ("**ISA**") is between Impero (as defined in Section 1), and the customer ordering the Impero Services/identified in the Service Order ("**Customer**" or "**you**").

1. DEFINED TERMS. The following words, when capitalized, have the meaning stated:

"**Affiliate**" means any legal entity that a party owns, that owns a party, or that is under its common ownership. "Ownership" means, for the purposes of this definition, control of more than a fifty percent interest in an entity.

"**Agreement**" means, collectively, this ISA and any applicable Service Order or other addenda which govern the provision of Services.

"**Business Day**" means Monday through Friday, excluding public holidays.

"**Confidential Information**" means non-public information disclosed by one party to the other in any form that: (i) is designated as "Confidential"; (ii) a reasonable person knows or reasonably should understand to be confidential; or (iii) includes either party's products, customers, marketing and promotions, know-how, or the negotiated terms of the Agreement; and which is not independently developed by the other party without reference to the other's Confidential Information or otherwise known to the other party on a non-confidential basis prior to disclosure.

"**Impero Platform**" means an information technology system provided and hosted by Impero as part of the Services, including any hosted platform or software as a service delivery of the Services.

"**Customer Data**" means all data which Customer (or its students, employees or end users) receive, store, or transmit on or using the Impero Platform.

"Data Protection Legislation" means unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then any successor legislation to the GDPR or the Data Protection Act 2018.

"**Deliverables**" means the tangible or intangible materials which are prepared for your use in the course of performing the Services (specifically excluding Device Agents).

"**Device Agents**" means any end-user or per-device software or agents provided by Impero to be used in conjunction with the Services.

"**End User Device**" means any individual computer or mobile device of any type which is used by Customer or its students, employees, or end users in connection with the Services or on which any Device Agent is installed.

"**Impero**" or "**we**" means the Impero Affiliate identified in the Service Order, or, if none is identified: (i) Impero Solutions, Inc. if your billing address is located in the United States or (ii) Impero Solutions LTD if your billing address is located outside of the United States.

"**Intellectual Property**" means patents, copyrights, trademarks, trade secrets, and any other proprietary intellectual property rights.

"**Sensitive Data"** means any: (i) personally identifiable information or information that is referred to as personal data (including sensitive personal data); PII (or other like term) under applicable data protection or privacy law and includes information that by itself or combined with other information can be used to identify a person; (ii) trade secrets; (iii) financial records; and (iv) other sensitive, regulated, or confidential information.

"**Impero Configuration Requirements**" means those specifications identified by Impero as required to perform the Services, including details regarding their interoperability, file structure requirements, and user access requirements.

"**Representatives**" means a party's respective service providers, officers, directors, employees, contractors, Affiliates, suppliers, and agents.

"**Services**" means the Impero services (including any software) identified in a given Service Order or otherwise provided subject to the terms of this Agreement, including access to the Impero Platform.

"**Service Order**" means the document which describes the Services provided pursuant to this Agreement, including any online order, process, or tool through which you request or provision Services.

2. SERVICES

2.1. General. Impero will provide the Services in accordance with the Agreement and all laws applicable to Impero. Customer must utilize the Services in accordance with any Impero provided documentation. Impero will provide support only to those individuals designated in your account and is not required to provide any support directly to your end users.

2.2. Usage Limitations. Customer may use the Services for educational, wellbeing, and other explicitly permitted purposes only, in accordance with all laws applicable to Customer, and may not resell the Services unless explicitly agreed to by Impero in writing.

2.3. Device Agents. During the term of the Agreement, Customer may use any software provided by Impero as part of the Services and may install Device Agents on its users' systems as necessary to receive the benefit of the Services. Device Agents may be subject to additional terms, including third party terms applicable to use of app stores for mobile devices. Customer is responsible for all use of Device Agents in connection with the Services. Fees for Device Agents will be specified on the Service Order where applicable.

3. CUSTOMER OBLIGATIONS

3.1. General. You must cooperate with Impero's reasonable investigation of outages, security problems, and any suspected breach of the Agreement. You are responsible for keeping your account information and permissions current. You agree that your use of the Services will comply with the Acceptable Use Policy attached as Exhibit A (the "**AUP**"). You agree that you are solely responsible for the suitability of the Services and your and your users' compliance with any applicable laws, including export laws and data privacy laws.

3.2. Data Backup. It is the Customer's responsibility to ensure the integrity and security of Customer Data and to regularly backup and validate the integrity of backups of Customer Data. Impero has no obligations whatsoever with regards to any data stored on an End User Device.

4. SECURITY. Impero undertakes no responsibility for the security of any End User Device. Customer must use reasonable security precautions in connection with its use of the Services. Customer Data is, and at all times shall remain, your exclusive property. Impero will not use or disclose Customer Data except as materially required to perform the Services or as required by law.

5. INTELLECTUAL PROPERTY

5.1. Pre-Existing. Each party shall retain exclusive ownership of Intellectual Property created, authored, or invented by it prior to the commencement of the Services. If you provide Impero with your pre-existing Intellectual Property ("**Customer IP**"), then you hereby grant to Impero, during the term of the applicable Service Order, a limited, worldwide, non-transferable, royalty-free, right and license (with right of sub-license where required to perform the Services) to use the Customer IP solely for the purpose of providing the Services. You represent and warrant that you have all rights in the Customer IP necessary to grant this license, and that Impero's use of such Customer IP shall not infringe on the Intellectual Property rights of any third party.

5.2. Created by Impero. Excluding any Customer IP, Impero shall own all Intellectual Property created as part of providing the Services or contained in the Deliverables. Unless otherwise specifically stated in the Agreement, and subject to your payment in full for the applicable Services, Impero grants to you, during the term of the applicable Service Order, a limited, non-exclusive, non-transferable, right and license (without the right to sublicense) to use any Deliverables, and any

Intellectual Property (including Device Agents, but excluding any Third Party Software), provided to you by Impero as part of the Services for your internal use as necessary for you to enjoy the benefit of the Services. You agree that any usage data, usage metrics, and other general information about your use or operation of the Services may be used and disclosed by Impero for product improvement and market analysis purposes.

5.3. Third Party Software. Impero may provide third party software for your use as part of the Services or to assist in our delivery of the Services ("**Third-Party Software**"). Unless otherwise permitted by the terms of the applicable license you may not: (i) assign, grant or transfer any interest in the Third Party Software to another individual or entity; (ii) reverse engineer, decompile, copy or modify the Third Party Software; (iii) modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Third Party Software; or (iv) exercise any of the reserved Intellectual Property rights provided under the laws governing this Agreement. Your use of any Third-Party Software may be subject to additional restrictions identified in the Service Order or an end-user license agreement or similar terms. Upon termination of the Service Order, you will remove any Impero provided software and Device Agents and any Third-Party Software which has been installed on your (or your users') devices. Impero makes no representation or warranty regarding Third Party Software except that Impero has the right to use or provide the Third-Party Software and that we are in material compliance with the applicable license.

5.4. Infringement. If the delivery of the Services infringes the intellectual property rights of a third party and Impero determines that it is not reasonably or commercially practicable to obtain the right to use the infringing element, or modify the Services or Deliverable such that they do not infringe, then Impero may terminate the Service Order on written notice and will not have any liability on account of such termination except to refund amounts paid for unused Services (prorated as to portions of Deliverables deemed infringing).

6. FEES.

6.1. Fees. Undisputed fees are due within 30 days of the invoice date. If you have arranged for payment by credit card or bank transfer, we may charge your account on or after the invoice date. If any undisputed payment is 15 or more days late, then we may suspend the Services on written notice. Invoices which are not disputed within 30 days of the invoice date are conclusively deemed accurate. Fees must be paid in the currency identified in the Service Order.

6.2. Fee Increases. On 90 days advance written notice, Impero may increase the fees due under any given Service Order by the greater of (i) 5% or (ii) the percentage change between the United Kingdom's Retail Price Index in the initial month of the applicable Service Order and the then current month, provided that Impero may not exercise these rights more than once in any 12 month period. If at any time a third party license or infrastructure provider directly or indirectly increases the fee they charge Impero for software or services required to deliver the Services, Impero may increase your fees by the same percentage amount on 90 days advance written notice.

6.3. Taxes. All amounts due to Impero under the Agreement are exclusive of any value added, goods and services, sales, use, property, excise and like taxes, import duties, and/or applicable levies (collectively "**Tax**"). You must pay any Taxes due on Impero's provision of the Services or provide Impero with valid evidence of your exemption from such Taxes in advance of invoicing. All fees are due in full without any deduction for any withholding or other taxes except withholding taxes imposed on income attributable to Impero which you are legally required to withhold and remit to the applicable governmental authority ("**Local Withholding Taxes**"). You agree to provide Impero with timely accurate information regarding such Local Withholding Taxes on request.

6.4. Expenses. Except as otherwise included in a given Service Order, if any of the Services are performed at your site or premises then you agree to reimburse Impero for the actual substantiated out-of-pocket expenses of our Representatives.

7. DISCLAIMERS

7.1. We make no commitment to provide any Services other than the Services stated in the Service Order. Impero is not responsible to you or any third party for unauthorized access to your Customer Data or for unauthorized use of the Services that is not solely caused by Impero's failure to comply with its security obligations in the Agreement.

7.2. At Customer's request Impero may provide Services that are not required by the Agreement, any such Services shall be provided AS-IS with no warranty whatsoever.

7.3. Impero and its Representatives disclaim any and all warranties not expressly stated in the Agreement to the maximum extent permitted by law including implied warranties such as merchantability, satisfactory quality, fitness for a particular purpose and non-infringement.

7.4. Impero makes no representation or warranty whatsoever regarding Open Source Software or with regard to any third-party products or Services which we may recommend for your consideration.

8. TERM AND TERMINATION

8.1. Term. This Agreement shall continue until terminated in accordance with its terms or the termination of the final Service Order, whichever is the later. Unless otherwise stated in the Service Order, Service Orders shall automatically renew following their initial term (identified on the Service Order) for consecutive one-year terms, unless and until either party provides the other with written notice of non-renewal at least 90 days prior to the expiration of the then current term.

8.2. Termination. Either party may terminate the Agreement or the affected Service Order(s) for cause on written notice if the other party materially breaches the Agreement and does not remedy the breach within 30 days of the other party's written notice describing the breach. If, following the suspension of your Services for non-payment as provided in Section 6.1 (Fees), your account remains overdue for a further 15 days, we may terminate the Agreement or the applicable Service Orders for breach on written notice. Where Impero terminates this Agreement for cause as provided for in this Section, all fees due for the then current term shall immediately become due and payable.

8.3. Transition. If you request contemporaneously with any notice of termination (by either party), Impero shall make the Customer Data available to you for a period of no more than 10 Business Days, in such format as it chooses. You agree that you shall promptly retrieve any Customer Data within this time period as required for you to comply with any applicable laws.

9. CONFIDENTIAL INFORMATION. Each party agrees not to use the other's Confidential Information except in connection with the performance or use of the Services, the exercise of its legal rights under this Agreement, or as required by law, and will use reasonable care to protect Confidential Information from unauthorized disclosure. Each party agrees not to disclose the other's Confidential Information to any third party except: (i) to its Representatives, provided that such Representatives agree to confidentiality measures that are at least as stringent as those stated in this Agreement; (ii) as required by law; or (iii) in response to a subpoena or court order or other compulsory legal process, provided that the party subject to such process shall give the other written notice of at least seven days prior to disclosing Confidential Information unless the law forbids such notice.

10. LIMITATIONS ON DAMAGES

10.1. Direct Damages. Notwithstanding anything in the Agreement to the contrary, except for liability arising from: (i) death or personal injury caused by negligence, (ii) willful misconduct, (iv) fraudulent misrepresentation or (v) any other loss or damages for which such limitation is expressly prohibited by applicable law, the maximum aggregate monetary liability of Impero and any of its Representatives in connection with the Services or the Agreement under any theory of law shall not exceed the total amount of fees paid for the Services in the twelve month period immediately preceding the event(s) giving rise to the claim.

10.2. Indirect Damages. Neither party (nor any of our Representatives) is liable to the other for any indirect, special, incidental, exemplary or consequential loss or damages of any kind. Neither of us is liable for any loss that could have been avoided by the damaged party's use of reasonable diligence, even if the party responsible for the damages has been advised or should be aware of the possibility of such damages. In no event shall either of us be liable to the other for any punitive damages or for any loss of profits, data, revenue, business opportunities, customers, contracts, goodwill or reputation.

11. INDEMNIFICATION

11.1. If we, our Affiliates, or any of our or their Representatives (the "**Indemnitees**") is faced with a legal claim by a third party arising out of your actual or alleged: willful misconduct, breach of applicable law, failure to meet the security obligations required by the Agreement, breach of your agreement(s) with or obligation(s) to your customers or end users, violation of the AUP, or your breach of Section 5 (Intellectual Property) then you will pay the cost of defending the claim (including reasonable legal fees) and any damages award, fine or other penalty that is imposed on the Indemnitees as a result of the claim. Your obligations under this Section include claims arising out of the acts or omissions of your employees or agents, any other person to whom you have given access to the Services, and any person who gains access to the Services as a result of your failure to use reasonable security precautions, even if the acts or omissions of such persons were not authorized by you.

11.2. We will choose legal counsel to defend the claim, provided that the choice is reasonable and is communicated to you. You must comply with our reasonable requests for assistance and cooperation in the defense of the claim. We may not settle the claim without your consent, which may not be unreasonably withheld, delayed or conditioned. You must pay costs and expenses due under this Section as we incur them.

12. NOTICES. Your routine communications to Impero regarding the Services should be sent to your account team using the customer portal. To give a notice regarding termination of the Agreement for breach, indemnification, or other legal matter, you must send it by electronic mail and first-class post to:

terminations@imperosoftware.com
Accounts Receivable
Impero Software
Oak House
Mere Way
Ruddington Fields Business Park
Ruddington
Nottingham
England
NG11 6JS

Impero's routine communications regarding the Services and legal notices will be sent by email or post to the individual(s) you designate as your contact(s) on your account. Notices are deemed received as of the time posted or delivered, or if that time does not fall within a Business Day, as of the beginning of the first Business Day following the time posted or delivered. For purposes of counting days for notice periods, the Business Day on which the notice is deemed received counts as the first day.

13. PUBLICITY, USE OF MARKS. Customer agrees that Impero may publicly disclose that it is providing Services to Customer and may use Customer's name and logo to identify Customer in promotional materials, including press releases. Customer may not issue any press release or publicity regarding the Agreement, use the Impero name or logo or other identifying indicia, or publicly disclose that it is using the Services without Impero's prior written consent.

14. ASSIGNMENT/SUBCONTRACTORS. Neither party may assign the Agreement or any Service Orders without the prior written consent of the other party except to an Affiliate or successor as part of a corporate reorganization or a sale of some or all of its business, provided the assigning party notifies the other party of such change of control. Impero may use its Affiliates or subcontractors to perform all or any part of the Services, but Impero remains responsible under the Agreement for work performed by its Affiliates and subcontractors to the same extent as if Impero performed the Services itself. Customer acknowledges and agrees that Impero Affiliates and subcontractors may be based outside of the geographic jurisdiction in which Customer is located.

15. FORCE MAJEURE. Neither party will be in violation of the Agreement if the failure to perform the obligation is due to an event beyond its control, such as significant failure of a part of the power grid, failure of the Internet, natural disaster or weather event, war, riot, insurrection, epidemic, strikes or labor action, terrorism, or other events beyond such party's reasonable control.

16. GOVERNING LAW

16.1. Impero Solutions, Inc. If you are contracting with Impero Solutions, Inc., then the Agreement is governed by the laws of the State of Texas, USA, exclusive of any choice of law principle that would require the application of the law of a different jurisdiction. Exclusive venue for all disputes arising out of the Agreement shall be in the state or federal courts in Travis County, Texas, and we each agree not to bring any action in any other venue. You waive all objections to this venue and agree not to dispute personal jurisdiction or venue in these courts.

16.2. Impero Solutions Ltd. If you are contracting with Impero Solutions Ltd, then the Agreement is governed by English law and each of us expressly and unconditionally submits to the exclusive jurisdiction of the courts of England and Wales.

16.3. No claim may be brought as a class or collective action, nor may you assert such a claim as a member of a class or collective action that is brought by another claimant. Each of us agrees that we will not bring a claim under the Agreement more than two years after the time that the claim accrued. The Agreement shall not be governed by the United Nations Convention on the International Sale of Goods.

17. HIPAA. If Impero is your Business Associate, as defined by 45 C.F.R. §160.103, then the Impero Business Associate Agreement attached as Exhibit B applies and is incorporated herein by reference.

18. FERPA. If Customer is an educational agency or institution to which regulations under the Family Education Rights and Privacy Act, 20 U.S.C. §1232g; 34 CFR § 99.33(a), as amended ("**FERPA**") applies, then Impero acknowledges that for purposes of the Services, Impero is a "school official" with "legitimate educational interests" in the Customer Data (as those terms are defined by FERPA and its implementing regulations), and Impero agrees to comply with the requirements of FERPA as they apply to school officials with legitimate educational interests. Customer is responsible for obtaining any parental consent for any end user's use of the Services that may be required by applicable law and to provide notification on behalf of Impero to students (or, a student's parent, as required) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Impero's possession as may be required under applicable law. You are responsible for addressing any records requests made by students or individuals entitled to access Customer Data subject to FERPA, provided that Impero will provide you with commercially reasonable assistance in fulfilling such requests. You are responsible for ensuring that your annual notification of FERPA rights includes the scope of the Services and this Agreement in the definition of "school official" and "legitimate educational interest."

19. COPPA. If the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §6501-6506 ("**COPPA**") applies to the Services, you are responsible for obtaining all student and/or parental consent as required by COPPA and must provide verifiable evidence of such consent upon our written request, provided that Impero will provide you with any reasonably requested information necessary to fulfill your obligations in obtaining consent. Where COPPA applies to Impero as part of its provision of the Services to Customer, Impero's information management practices are attached as Exhibit C.

GDPR

19.1. If we collect "Personal Data" as defined by the Data Protection Legislation as part of delivering the Services to you, then the Impero Data Protection Policy (attached as Exhibit D) and the Impero Data Retention Policy (attached as Exhibit E) apply and are incorporated herein by reference. In so far as required, both you and we agree that we will comply with all applicable requirements of the Data Protection Legislation. This clause is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

19.2. You acknowledge that for the purposes of the Data Protection Legislation, you are the data controller and Impero is the data processor (where Data Controller and Data Processor have the meanings as defined in the Data Protection Legislation). The Impero Data Protection Policy and Impero Data Retention Policy set out the scope, nature and purpose of processing by Impero, the duration of the processing and the types of Personal Data (as defined in the Data Protection Legislation, Personal Data) and categories of Data Subject.

19.3. As the Processor for the Personal Data, Impero will only process Personal Data provided by you or any user (i) in accordance with your written instructions (including this ISA) or (ii) where required to do so by applicable law.
19.4. Without prejudice to the generality of clause 20.3, you will ensure that you have all necessary appropriate consents and notices in place to enable lawful transfer of any required Personal Data to Impero for the duration and purposes of this agreement.
19.5. Without prejudice to the generality of clause 20.3, Impero warrants and undertakes that it shall, in relation to any Personal Data processed in connection with the performance by Impero of its obligations under this ISA:
(a) process that Personal Data only on your written instructions unless we are required by the laws of any member of the European Union or by the laws of the European Union applicable to Impero to process Personal Data (Applicable Laws). Where Impero is relying on laws of a member of the European Union or European Union law as the basis for processing Personal Data, we shall promptly notify you of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit us from so notifying you;
(b) ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);
(c) ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential; and
(d) not transfer any Personal Data outside of the European Economic Area unless the prior written consent of Customer has been obtained (and the following conditions are fulfilled:
(i) Impero has provided appropriate safeguards in relation to the transfer;
(ii) the data subject has enforceable rights and effective legal remedies;
(iii) Impero complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
(iv) Impero complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;
(e) assist you, at your cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
(f) notify you without undue delay on becoming aware of a Personal Data breach;
(g) Personal Data will be processed for the duration of this Contract. Upon termination of the Contract, you shall be given the option to have all Personal Data securely deleted or, upon your request, returned to you (in a format specified by Impero), unless applicable law prevents us from returning or destroying all or part of the Personal Data. If you choose not to request the deletion of this Personal Data, the Personal Data will be archived and retained for a maximum period of 7 years, after which the Personal Data is deleted.
19.6. You shall own all right, title and interest in and to all of the Customer Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Customer Data.
19.7. Impero shall, in providing the Services, comply with its IT Security measures relating to the privacy and security of the Customer Data.

20. MISCELLANEOUS
20.1. Unless otherwise expressly permitted in the Agreement the terms of the Agreement may be varied only by a written agreement signed by both parties that expressly refers to the Agreement. A Service Order may be amended to modify, add, or remove Services by a formal written agreement signed by both parties, or by an exchange of correspondence (including via the Impero customer management system) that includes the express consent of an authorized individual for each of us. The pre-printed terms of your purchase order or other business form or terms that you provide shall be void and of no effect.

20.2. If any part of the Agreement is found unenforceable, the rest of the Agreement will continue in effect, and the unenforceable part shall be reformed to the extent possible to make it enforceable and give business efficacy to the Agreement. Each party may enforce its respective rights under the Agreement even if it has waived the right or failed to enforce the same or other rights in the past. The relationship between the parties is that of independent contractors and not business partners. Neither party is the agent for the other and neither party has the right to bind the other on any agreement with a third party. The use of the word “including” means “including without limitation”. Other than Representatives for the purposes of Sections 7, 10, and 11, there are no third-party beneficiaries to the Agreement.

20.3. The following provisions shall survive expiration or termination of this Agreement: Intellectual Property, Confidential Information, Indemnification, Limitation on Damages, Governing Law, Notices, Miscellaneous, all terms of the Agreement requiring you to pay any fees for Services provided prior to the time of expiration or termination, or requiring you to pay an early termination fee, and any other provisions that by their nature are intended to survive expiration or termination of the Agreement.

20.4. The Agreement constitutes the complete and exclusive understanding between the parties regarding its subject matter and supersedes and replaces any prior or contemporaneous representation(s), agreement(s) or understanding(s), written or oral.

EXHIBIT A
ACCEPTABLE USE POLICY

Your use of the Services is subject to this Acceptable Use Policy (this "**AUP**"), and you are responsible for ensuring that your users and anyone you give access to the Services complies with this AUP and the Agreement. We may update this AUP over time as we deem necessary and appropriate in response to legal or regulatory changes, technology advances, or as we identify new forms of behavior which pose a risk to our users, shared systems, or is inconsistent with our or our customer's legal obligations.

1. You may not use the Services to engage in, foster, or promote illegal, abusive, or irresponsible behavior.

2. Except to the extent that such content is educational content or is necessary for the purposes of safeguarding the wellbeing of students in a lawful manner, you may not publish, transmit, or store on or via the Services any content or links to any content that:
   - Constitutes, depicts, fosters, promotes, or relates in any manner to any sexual activity.
   - Is excessively violent, incites violence, threatens violence, contains harassing content or hate speech.
   - Is unfair or deceptive.
   - Is defamatory or violates a person's privacy.

3. You may not attempt to probe, scan, penetrate, or test the vulnerability of an Impero system or network, or to breach the Impero security or authentication measures in any form (actively or passively).

4. You may not use the Services in a manner that infringes on or misappropriates the rights of a third party in any work protected by copyright, trade or service mark, invention, or other intellectual property or proprietary information. It is Impero's policy to terminate customers who are repeat infringers in appropriate circumstances.

EXHIBIT B
BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Association Agreement (this "**BAA**") is an addendum to your Agreement (and incorporated therein by reference). This BAA defines the rights and responsibilities of each of us with respect to Protected Health Information as defined in the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder, including the HITECH Act and Omnibus Rule, as each may be amended from time to time (collectively, "**HIPAA**"). This BAA shall be applicable only in the event and to the extent Impero meets, with respect to you, the definition of a Business Associate set forth at 45 C.F.R. §160.103, or applicable successor provisions.

1. Defined Terms. For the purposes of this BAA, capitalized terms shall have the following meanings, and otherwise as defined in the Agreement:

"**Business Associate**" shall mean Impero.

"**Individual**" shall have the same meaning as the term "individual" in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

"**Privacy Rule**" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

"**Protected Health Information**" or "**PHI**" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information received by Business Associate from or on behalf of Customer.

"**Required By Law**" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

"**Security Rule**" shall mean the Security Standards for the Protection of Electronic Protected Health Information, located at 45 CFR Part 160 and Subparts A and C of Part 164.

"**Secretary**" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

2. Obligations and Activities of Business Associate.

(a) Business Associate shall not use or disclose Protected Health Information other than as permitted or required by this BAA or as permitted or Required by Law.

(b) Business Associate agrees to provide those physical, technical and administrative safeguards described in the Agreement including those safeguards and services selected by you and described in a Service Order. If Business Associate agrees as part of this BAA to carry out an obligation of yours under the Privacy Rule, then Business Associate will comply with the requirements of the Privacy Rule applicable to such obligation.

(c) Business Associate agrees to mitigate, to the extent commercially reasonable and reasonably practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate or its agents or subcontractors in violation of the requirements of this BAA.

(d) Within five Business Days of becoming aware, Business Associate agrees to report to you (i) Security Incidents (as defined in 45 C.F.R. §164.304 and as further described below), (ii) the Breach of unsecured PHI (as defined in 45 CFR §164.402), or (iii) an access, acquisition, use or disclosure of PHI in violation of this BAA.

(1) Both parties acknowledge that there are likely to be a significant number of meaningless or unsuccessful attempts to access the Services, which make a real-time reporting requirement impractical for both parties. The parties acknowledge that Business Associate's ability to report on system activity, including Security Incidents, is limited by, and to, Customer's specific Services and instances thereof, and does not include End User Devices.

(2) Business Associate undertakes no obligation to report unsuccessful security incidents or to report network security related incidents which occur on the Impero managed network or systems but do not directly involve Customer Data. The parties agree that the following are illustrative examples of unsuccessful security incidents which, when they do not result in the unauthorized access, use, disclosure, modification or destruction of PHI need not be reported by Business Associate: pings against network devices, port scans, attempts to log on to a system or database with an invalid password or username, malware.

(e) Business Associate agrees to obtain from any agent, including a subcontractor to whom it provides Protected Health Information, reasonable assurances that it will adhere to the same restrictions and conditions that apply to Business Associate under this BAA with respect to such information.

(f) All Protected Health Information maintained by Business Associate for you will be available to you in a time and manner that reasonably allows you to comply with the requirements under 45 CFR § 164.524. Business Associate shall not be obligated to provide any such information directly to any Individual or person other than you.

(g) All Protected Health Information and other information maintained by Business Associate for you will be available to you in a time and manner that reasonably allows you to comply with the requirements under 45 CFR § 164.526.

(h) Business Associate agrees to make internal practices, books, and records available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary's determining your compliance with the Privacy Rule; provided, however, that time incurred by Business Associate in complying with any such request that exceeds its normal customer service parameters shall be charged to you at Business Associate's then current hourly rate for additional services.

(i) You acknowledge that Business Associate is not required by this BAA to make disclosures of Protected Health Information to Individuals or any person other than you, and that Business Associate does not, therefore, expect to maintain documentation of such disclosure as described in 45 CFR § 164.528. In the event that Business Associate does make such disclosure, it shall document the disclosure as would be required for you to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR §164.504(e)(2)(ii)(G) and §164.528, and shall provide such documentation to you promptly on your request. In the event that a request for an accounting is made directly to Business Associate, Business Associate shall, within 2 Business Days, forward such request to Customer.

3. Permitted Uses and Disclosures by Business Associate. Except as otherwise limited by this BAA or other portion of the Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or Services for, or on behalf of, you as specified in the Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by you.

4. Specific Use and Disclosure Provisions. Except as otherwise limited in this BAA or other portion of the Agreement, Business Associate may:

(a) use Protected Health Information for the proper management and administration of Business Associate or to carry out its legal responsibilities;

(b) disclose Protected Health Information for the proper management and administration of Business Associate, provided that disclosures are (i) Required By Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person will notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached; and

(c) use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1).

5. Your Obligations. You shall notify Business Associate of:

(a) any limitations(s) in your notice of privacy practices in accordance with 45 CFR § 164.520 to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information;

(b) any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information; and

(c) any restriction to the use or disclosure of Protected Health Information that you have agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.
You agree that you will not request that Business Associate use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by you.

You agree to comply with those security obligations identified in the Agreement, and to implement or maintain appropriate safeguards and practices as required for you to comply with the Security and Privacy rules as applicable to you.

6. Term and Termination

(a) The term of this BAA shall continue for the term of the Agreement to which this BAA is incorporated by reference, and following termination of such Agreement until all Protected Health Information is destroyed or returned to you or your designee.

(b) If Business Associate materially breaches the terms of this BAA, then you may terminate any related Agreements(s).

(c) Upon termination of the Agreement for any reason Business Associate shall destroy all Protected Health Information which remains on the Impero Platform or otherwise in Business Associates possession. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate as well as Business Associate itself. Business Associate shall retain no copies of the Protected Health Information. In the event that Business Associate determines that destroying the Protected Health Information is infeasible, Business Associate shall promptly provide you notification of the conditions that make destruction infeasible. Business Associate shall extend the protections of this BAA to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the destruction infeasible, for so long as Business Associate maintains such Protected Health Information. You shall bear the cost of storage of such Protected Health Information for as long as storage by Business Associate is required. This Section does not require Business Associate to segregate any Protected Health Information from other information maintained by you on Business Associate's servers and Business Associate may comply with this requirement by deleting all of the Protected Health Information received from you and maintained on the Impero Platform or Business Associate's systems.

(d) If you request contemporaneously with any termination event or notice, Business Associate will allow you to have access to your Customer Data a reasonable period of time following termination as necessary for you to retrieve or delete any Protected Health Information at your then current fees; provided, however, that if the Agreement was terminated for your breach of the AUP or the Agreement, Impero may: (i) provide you with restricted access via a private link to your Customer Data or (ii) use reasonable efforts to copy your data on to media you provide to Impero, and will ship the media to you at your expense. Impero's efforts to copy your data onto your media shall be billable at Impero's then current hourly rates.

7. Miscellaneous.

(a) Amendment. Each of us agrees to take such action as is reasonably necessary to amend this BAA from time to time as is necessary for you to comply with the requirements of HIPAA as they may be amended from time to time; provided, however, that if such an amendment would materially increase the cost of Business Associate providing service under the Agreement, Business Associate shall have the option to terminate the Agreement on thirty (30) days advance notice. Any ambiguity in this BAA shall be resolved to permit you to comply with HIPAA and the Privacy Rule.

(b) Survival. Our respective rights and obligations under this BAA shall survive the termination of the Agreement.

EXHIBIT C
NOTICE OF COPPA PRACTICES

Impero Solutions, Inc. ("**Impero**") provides its customer educational institutions ("**Schools**") with cloud-based services which enable the Schools to administer their systems, student systems, track student progress and welfare concerns, enhance School staff collaboration, and organize student information (the "**Services**"). Consistent with our obligations under the FTC's Children's Online Privacy Protection Act ("**COPPA**") we provide this Notice of COPPA Practices (this "**Notice**") to better assist Schools, students, parents, and teachers in understanding how we receive, store, and manage the information we collect in the Services.

1. Consent. Impero relies on Schools to obtain consent from parents for the collection and use of personal information of Students (of any age), in compliance with FERPA and their local legal and policy requirements.

2. Impero's Required Notices Under COPPA. Impero is required by COPPA to provide the following information, which Schools may also provide to their students and parents in order to effectively inform the consent requirements under laws applicable to the School. The rest of this Notice is designed to provide further information to Schools, students, and parents about how information collected by the Services is used.

2.1. Collection & Contact Information. Impero collects and maintains any personal information received through the Services. Impero may utilize subcontractors and its affiliates to assist it in the delivery of the Services, including for purposes of storing personal information received through the Sites and Services. As of the date of this Notice, Impero utilizes Microsoft's Azure Cloud to host elements of the Sites and Services and Impero's UK affiliate, Impero Solutions LTD may assist in the delivery of the Site and Services. Impero handles all requests relating to its provision of the Services. Impero will respond to any inquiries from a School or Parent directed to: edaware@imperosoftware.com.

2.2. Information Collected & Disclosure Practices. Impero makes use of the information collected in order to provide the Services to Schools as agreed in their given service orders, and for no other commercial purpose.

Children *can not* choose to make their information publicly available, although they can provide information to teachers and the School using the Services.

Impero does not disclose collected information other than to the School, to our subcontractors as necessary to provide the Services in accordance with applicable law, or as required to respond to valid legal process issued by a court of competent jurisdiction.

The information collected by Impero varies by product and by School based on the specific implementation and selected usage. Each Impero service may collect common information about devices and users including names, online contact (username/email), last known IP address, and the machine name of the device last used. Example categories are detailed below by Service:

- **Impero EdProtect:** Monitoring of devices and usage to identify inappropriate behavior and technical issues, keyword detection and monitoring, online activity logging, context capture (screenshot/video recording), self-submitted student information.
- **Impero EdLink:** Monitoring of devices and usage to identify inappropriate behavior and technical issues, utilization monitoring, student identification and device usage, geolocation data, internet usage (including to enable filtering controls).
- **Impero EdTeach:** Student name and identity, testing administration, curriculum completion, active viewing of current device usage, messaging and live chat content.
- **Impero EdAware:** Student profile and demographic information, full name, welfare history, medical history, sibling identity, home address, persistent identifiers, student images.
- **Impero EdAdmin:** Monitoring of devices and usage to identify inappropriate behavior and technical issues, utilization monitoring, student identification and device usage.

2.3. Review & Deletion. Schools and parents may review or have children's personal information deleted and may refuse to permit further collection or use of a child's information. If you are a parent and have concerns, we suggest that you contact your child's School or teacher so that they can respond directly to your concerns. You may also contact Impero as identified above. Impero may engage in validation procedures, including relaying your request to the School, in order to protect collected information from unauthorized disclosure or deletion.

3. What Types of Information Does Impero Collect from Students? This varies by both the Services purchased and a School's implementation of those Services. Please see the lists above in Section 2.2 (Information Collected & Disclosure Practices) for details by Impero Service.

4. How Does Impero Use this Personal Information? Impero uses the collected personal information solely for the purposes of providing the Sites and Services to the School, in accordance with the agreement with the School and applicable law.

5. Does Impero Use or Share the Information for Commercial Purposes Not Related to the Provision of the Services Requested by the Customer? No. Impero only collects and uses personal information collected from students for the use and benefit of the School and for no other purpose. This enables Schools to obtain consent directly from parents. We require that Schools provide administrative contacts authorized to consent on behalf of parents and implement identity management controls to ensure that the School officials are providing the consent (and not a student pretending to be a teacher, for example).

6. Does Impero Enable the School to Review and Have Deleted the Personal Information Collected From Their Students? Yes. Schools remain directly in control of the majority of information collected by the Services and are the primary administrator of such data. Where Impero's Services also collect usage data or similar analytics which are presented to the School, Impero will provide review of the raw data to the School upon their request and will delete such information upon the Schools request.

7. What Measures Does Impero Take to Protect the Security, Confidentiality, and Integrity of the Personal Data that it Collects? Impero implements administrative, technical, and physical access controls designed to protect the security, confidentiality, and integrity of the personal data it collects, the systems which store such personal data, and the locations in which such data or systems are stored.

As a global provider of educational technology services and solutions, Impero takes data security and privacy seriously and complies with the EU General Data Protection Regulation (the "**GDPR**") where applicable. The controls required to comply with the GDPR are implemented throughout Impero's service delivery model.

8. What are Impero's Data Retention and Deletion Policies for Children's Personal Information? As a global provider of educational technology services and solutions, Impero takes data security and privacy seriously and complies with the GDPR where applicable. The controls required to comply with the GDPR are implemented throughout Impero's service delivery model. In addition, Impero will delete any personal information of Student's as requested by a School or parent pursuant to COPPA or other applicable law.

9. What is the Date of this Notice / When Was it Last Revised? This Notice is current as of January 22, 2019.

EXHIBIT D
DATA PROTECTION POLICY

1. INTRODUCTION

1.1. You have legal rights with regard to the way your personal data is handled. In the course of our business activities we collect, store and process personal data about our customers, suppliers and other third parties, and therefore in order to comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful treatment of this data. All people working in or with our business are obliged to comply with this policy when processing personal data.

1.2. This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from Data Subjects, for example, customers and business contacts, or that is provided to us by Data Subjects or other sources.

1.3. It also sets out our obligations in relation to data protection under the General Data Protection Regulation ("the Regulation").

1.4. This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data. The procedures and principles set out herein must be followed at all times by us and our employees, agents, contractors, or other parties working on behalf of the Company.

1.5. We aim to ensure the correct, lawful, and fair handling of your personal data and to respect your legal rights.

2. TERMINOLOGY

2.1. Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

2.2. Data Subjects for the purpose of this policy include all living individuals about whom we hold personal data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their personal information.

2.3. Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

2.4. Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

2.5. Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties. We are the data processor of all personal data provided by our customers.

3. THE COMPANY'S ROLE AS A DATA CONTROLLER

3.1. The Company shall ensure that the following information is provided to every Data Subject when personal data is collected or in advance of data collection:

- **a)** Details of the Company including, but not limited to, the identity of its Data Protection Officer.
- **b)** The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;
- **c)** Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
- **d)** Where the personal data is not obtained directly from the Data Subject, the categories of personal data collected and processed;
- **e)** Where the personal data is to be transferred to one or more third parties, details of those parties;
- **f)** Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place;
- **g)** Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);
- **h)** Details of the Data Subject's rights under the Regulation;
- **i)** Details of the Data Subject's right to withdraw their consent to the Company's processing of their personal data at any time;

j) Details of the Data Subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

3.2. The information set out above shall be provided to the Data Subject at the following applicable time:

a) Where the personal data is obtained from the Data Subject directly, at the point of collection, or in advance of collection;

b) Where the personal data is not obtained from the Data Subject directly (i.e. from another party):

c) If the personal data is used to communicate with the Data Subject, at the time of the first communication; or

d) If the personal data is to be disclosed to another party, before the personal data is disclosed; or

e) In any event, not more than one month after the time at which the Company obtains the personal data.

3.3. A Data Subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the Data Subject shall be informed of the need for the extension).

3.4. All subject access requests received must be forwarded to Nick Broadhurst, the Company's data protection officer. The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a Data Subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

3.5. If a Data Subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the Data Subject informed of that rectification, within one month of receipt the Data Subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the Data Subject shall be informed of the need for the extension). In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

3.6. Data Subjects may request that the Company erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;

b) The Data Subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) The Data Subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so);

d) The personal data has been processed unlawfully;

e) The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

3.7. Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the Data Subject informed of the erasure, within one month of receipt of the Data Subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the Data Subject shall be informed of the need for the extension). In the event that any personal data that is to be erased in response to a Data Subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

3.8. Data Subjects may request that the Company ceases processing the personal data it holds about them. If a Data Subject makes such a request, the Company shall retain only the amount of

personal data pertaining to that Data Subject that is necessary to ensure that no further processing of their personal data takes place. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

4. THE COMPANY'S ROLE AS A DATA PROCESSOR

4.1. The Company processes information on behalf of its customers, including personal data and special personal data, under the following bases:

- **a)** explicit consent from the Data Controller;
- **b)** a contract between the Company and the Data Controller;
- **c)** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
- **d)** processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child.

4.2. The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to the Data Controller. It is the responsibility of the Data Controller to make the Data Subjects aware of this data processing.

4.3. The Company, to the fullest extent possible, shall provide the means to ensure that all personal data collected and processed is kept accurate and up-to-date, but this ultimate responsibility will lie with the Data Controller.

4.4. When requested by the Data Controller, the Company will erase any data belonging to the Data Controller held on its systems.

4.5. If the Company receives a SAR or data portability request from a Data Subject where data is controlled by the Data Controller, this will be forwarded to the Data Controller at the earliest available opportunity.

4.6. Upon receiving a data portability request or SAR from a Data Controller, the Company will respond to this as soon as practicable and in any event within ten working days.

5. DATA PORTABILITY

5.1. Where Data Subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the Data Subject, Data Subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other Data Controllers, e.g. other organisations).

5.2. To facilitate the right of data portability, the Company shall make available all applicable personal data to Data Subjects or Data Controllers in the following format:

- **a)** For scanned information or information which the company does not hold in an editable format, PDF or image file;
- **b)** For written information in which the company holds it in an editable format, as a docx, rtf or pages file;
- **c)** For tabular information in which the company holds it in an editable format, as a xlsx, csv or numbers file;
- **d)** For information retrieved from a database, as a csv or sql file.

5.3. Where technically feasible, if requested by a Data Subject, personal data shall be sent directly to another Data Controller.

5.4. All requests for copies of personal data shall be complied with within one month of the Data Subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the Data Subject shall be informed of the need for the extension).

6. DATA SECURITY

6.1. The Company shall implement reasonable and appropriate controls designed to help ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

6.2. The Company has measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to

demonstrate compliance with the Regulation. Further details of these can be provided to Data Subjects and Data Controllers on request.

7. OBJECTIONS

7.1. Data Subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

7.2. Where a Data Subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the Data Subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

7.3. Where a Data Subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.

7.4. Where a Data Subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the Data Subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

8. PRIVACY IMPACT ASSESSMENTS

8.1. The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Company's data protection officer and shall address the following areas of importance:

- **a)** The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
- **b)** Details of the legitimate interests being pursued by the Company;
- **c)** An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

9. ACCOUNTABILITY

9.1. The Company's data protection officer is Nick Broadhurst.

10. ORGANISATIONAL MEASURES

10.1. All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy.

10.2. Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

10.3. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.

10.4. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised.

10.5. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.

10.6. The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

10.7. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract.

10.8. All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation.

10.9. Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

11. DATA BREACH NOTIFICATION

11.1. All personal data breaches must be reported immediately to the Company's data protection officer by email to infosec@imperosoftware.com.

11.2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

11.3. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 27.2) to the rights and freedoms of Data Subjects, the data protection officer must ensure that all affected Data Subjects are informed of the breach directly and without undue delay.

11.4. Data breach notifications shall include the following information:

- **a)** The categories and approximate number of Data Subjects concerned;
- **b)** The categories and approximate number of personal data records concerned;
- **c)** The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
- **d)** The likely consequences of the breach;
- **e)** Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

12. INTERNATIONAL TRANSFERS

12.1. The Company shall only store and transfer personal data in the United Kingdom except where set out in Schedule 1.

13. IMPLEMENTATION

13.1. This Policy shall be deemed effective as of 1st May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

SCHEDULE 1 to EXHIBIT D: INTERNATIONAL TRANSFERS OF DATA

The current list of the Company's hosting locations (which the Company uses to store sensitive personal data), as well as the international systems which, for operational reasons, the Company uses as data processors, are available at:

https://www.imperosoftware.com/uk/policies-terms/

EXHIBIT E
DATA RETENTION POLICY

1. Introduction

This Policy sets out the obligations of Impero Solutions Limited, a company registered in the UK under number 06106013, whose registered office is at Oak House, Mere Way, Ruddington Fields Business Park, Nottingham, NG11 6JS ("the Company") regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
b) When the data subject withdraws their consent;
c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;
d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);
e) When the personal data has to be erased to comply with a legal obligation; or
f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company's Data Protection Policy.

2. Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1 This Policy applies to all personal data held by the Company and by third-party data processors processing personal data on the Company's behalf.

3.2 Personal data, as held by the Company is stored in the following ways and in the following locations:

a) The Company's servers, located in Oak House, Ruddington (Head Office address);
b) Computers permanently located in the Company's premises at Oak House, Ruddington (Head Office address);
c) Laptop computers and other mobile devices provided by the Company to its employees;
d) Computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with the Company's Bring Your Own Device ("BYOD") Policy;
e) Physical records stored in Oak House, Ruddington (Head Office address)

4. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

4.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used as set out in the Company's Data Protection Policy, and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, as set out in the Company's Data Protection Policy.

5. Data Security Measures

5.1 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details:

a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;
b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;
c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;
e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR where applicable and controls consistent with the Company's Data Protection Policy;
i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted;

6.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted;

6.3 Personal data stored in hardcopy form shall be shredded

7. Data Retention

7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Company;
b) The type of personal data in question;
c) The purpose(s) for which the data in question is collected, held, and processed;
d) The Company's legal basis for collecting, holding, and processing that data;
e) The category or categories of data subject to whom the data relates;

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Types of personal data

As may be provided by the Customer from time to time, including but not limited to:

- Names
- Surnames
- Addresses
- Email addresses
- Telephone numbers
- Date of birth

- Marital status
- Occupation

Other types of Personal Data as may be submitted by the Customer to the Company from time to time to enable the Company to provide the Services under this Contract.

Categories of data subject

Some special categories of Personal Data may be processed from time to time, as directed by the Customer to the Company. These may specifically include:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

Other types of special category Personal Data as may be submitted by the Customer to the Company from time to time to enable the Company to provide the Services under this Contract.