Jisc Agreement for Software as a Service

between Jisc Services Ltd and Boxphish Ltd for Cyber Security Awareness Training & Phishing Simulations

20 August 2025

Schedule 5: The Licensor/Supplier's Data Protection Arrangement

Boxphish Data Processing Agreement (DPA)

Boxphish may update this DPA from time to time. Customers will be notified via email when we update this DPA.

1. Definitions

In this DPA, unless the text specifically notes otherwise, the below words shall have the following meanings:

Controller, Processor, Data Subject, Personal Data, Personal Data Breach, processing and appropriate technical and organisational measures shall be as defined in the Data Protection Legislation, where **Data Protection Legislation** means all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

License Agreement means the agreement between the Processor and the Controller to which this DPA is appended.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Sub-Processor means any person or entity appointed by or on behalf of the Processor to process personal data on behalf of the Controller.

2. Terms of Agreement

This DPA supplements the License Agreement and makes legally binding provisions for compliance with the Data Protection Legislation. As per the requirements of the Data Protection Legislation, all processing of personal data by a Processor (Boxphish) on behalf of a Controller (the Customer), shall be governed by a contract. The terms, obligations and rights set forth in this DPA relate directly to the data processing activities and conditions set out in Schedule 1.

3. Rights and Obligations of the parties

3.1 Both parties shall comply with the Data Protection Legislation. This DPA is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

3.2 The parties acknowledge that:

a) Schedule 1 sets out the scope, nature and purpose of processing by the Processor, the duration of the processing and the types of personal data and categories of Data Subject.
b) the Personal Data may be transferred or stored outside the EEA or the country where the Controller is located in order to carry out the Service and the Processor's other obligations under this DPA.
c) without prejudice to the generality of clause 3.1, the Controller will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Processor for the duration and purposes of this DPA so that the Processor may lawfully use, process and transfer the Personal Data in accordance with this DPA on the Controller's behalf.

d) without prejudice to the generality of clause 3.1, the Processor shall, in relation to any Personal Data processed in connection with the performance by the Processor of its obligations under this DPA:

i. process that Personal Data only on the written instructions of the Controller unless the Processor is required by the laws applicable to the Processor to process Personal Data (**Applicable Laws**). Where the Processor is relying on Applicable Laws as the basis for processing Personal Data, the Processor shall promptly notify the Controller of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Processor from so notifying the Controller;

ii. ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the Controller, 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);

iii. ensure that any personnel engaged and authorised by the Processor to process such Personal Data have committed themselves to confidentiality or are under an appropriate statutory or common law obligation of confidentiality;

iv. not transfer any Personal Data outside of the UK or EEA unless the following conditions are fulfilled:

- the Controller or the Processor has provided appropriate safeguards in relation to the transfer;
- the Data Subject has enforceable rights and effective legal remedies;
- the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
- the Processor complies with reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data.

v. assist the Controller, at the Controller's 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;

vi. at the written direction of the Controller, delete or return Personal Data and copies thereof to the Controller on termination of the License Agreement unless required by Applicable Laws to store the Personal Data;

vii. maintain complete and accurate records and information to demonstrate its compliance with this clause 3.2 and allow for reasonable audits by the Controller or the Controller's designated auditor, for this purpose, on reasonable written notice; and

viii. where applicable, employ a Data Protection Officer if required.

e) Either party may, at any time on not less than 30 days' notice, revise this clause 3.2 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when replaced by attachment to this DPA).

3.3 The Processor shall ensure that where a Sub-Processor is used, they: -

a) only engage a Sub-Processor with the prior consent of the Controller (and the Controller hereby consents to the use of the Sub-Processors listed in Schedule 2).
b) inform the controller of any intended changes concerning the addition or replacement of Sub-Processors
c) have entered or (as the case may be) will enter with the Sub-Processor into a written agreement incorporating terms which are substantially similar to those set out in this clause 3. As between the Controller and Processor, the Processor shall remain liable for all acts or omissions of any Sub-Processor appointed by it pursuant to this clause 3.3.
d) assist the Controller in providing subject access and allowing data subjects to exercise their rights under the Data Protection Legislation. If the Processor receives a request for an individual right directly from an individual, the Processor shall forward the request to the Controller within five (5) days and await written instructions from the Controller on how, if at all, to assist in responding to the request.
e) assist the Controller in meeting its data protection obligations in relation to:
    i. the security of processing;
    ii. data protection impact assessments; and
    iii. the investigation and notification of Personal Data Breaches as set forth herein.

3.4 The Processor shall comply with the Personal Data Breach-related obligations directly applicable to it under the Data Protection Legislation and, taking into account the nature of processing and the information available to the Processor, shall assist Controller in complying with those applicable to Controller, including by:

i. notify the Controller without undue delay on becoming aware of a Personal Data breach;
ii. within such time period, and without undue delay as the information becomes available after that (and in any event at least once each day that there is new information), informing Controller of the following (and of any reasonably available information that could help Controller independently assess the following):
    - The nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
    - The likely consequences of the Personal Data Breach; and
    - Measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; and
    - promptly providing the Controller with other information and records sufficient to document the Controller's and the Processor's compliance with the Personal Data Breach-related requirements of Applicable Laws; and
    - following a Personal Data Breach, providing reasonable assistance and cooperation to Controller to take measures that in Controller's reasonable determination (i) reduce the risk to individuals whose Personal Data was involved, or (ii) otherwise help Controller qualify for an exemption from a legal requirement to notify an individual or a supervisory authority of the Personal Data Breach.

3.5 The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller, containing:

a) the name and contact details of the Processor;
b) the categories of processing carried out on behalf of each Controller;
c) transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, the documentation of suitable safeguards; and
d) a general description of the technical and organisational security measures referred to in Article 32(1) of the GDPR.

3.6 The Processor shall maintain records of processing activities in electronic form and shall make the record available to Controller or applicable supervisory authority in coordination with Controller, on request.

3.7 When assessing the appropriate level of security and the subsequent technical and operational measures, the Processor shall consider the risks presented by any processing activities, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

4. Relationship with the License Agreement

4.1 Except for any variations made by this DPA, the License Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the License Agreement, this DPA shall prevail to the extent of that conflict.

4.2 Any claims against the Processor under this DPA shall be brought solely against the entity that is a party to the License Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. The Controller further agrees that any regulatory penalties incurred by the Processor in relation to the Personal Data that is caused by the Controller's failure to comply with its obligations under this DPA or any applicable Data Protection Legislation shall count toward and reduce the Processor's liability under the principal contract as if it were liability to the controller under the principal contract.

4.3 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

5. General

5.1 This DPA applies where and only to the extent that the Processor processes Personal Data that is subject to Data Protection Legislation on behalf of the Controller as Data Processor in the course of providing Services pursuant to the License Agreement.

5.2 The Controller agrees that it has provided notice and obtained (or shall obtain) all legal bases necessary under Data Protection Legislation for the Processor to process the Personal Data and provide the Service pursuant to the License Agreement.

5.3 The provisions of this DPA shall survive the termination or expiration of the License Agreement for so long as the Processor or its direct or indirect subcontractors have custody, control or possession of the Personal Data.

5.4 The Controller may disclose this DPA and a copy of the relevant privacy and security provisions of the License Agreement to a regulator or Controller customer if required by Applicable Laws or by contract provisions that the Controller entered into with its customers or third parties to legitimise the transfer of the Personal Data from the customer or third party to the Controller under Applicable Laws.

SCHEDULE 1

1. Processing Details

a) The Controller named in this DPA has appointed the Processor with regard to specific processing activity requirements. These requirements relate to provision of the Software and Service.

b) The duration of the data processing under this DPA is until the termination of the License Agreement in accordance with its terms.

c) The purpose of the data processing under this DPA is the provision of the Processor's Service and Software and the performance of the Processor's obligations under the License Agreement and this DPA or as otherwise agreed by the parties.

d) The nature of the processing is the provision of cyber security educational services.

e) The requirement for the Processor to act on behalf of the Controller is with regard to the below type(s) of Personal Data and categories of Data Subjects:

   i. Controller and User (as defined below) data including: identification and contact data (name, date of birth, gender, occupation or other demographic information, address, title, contact details (including email address), personal interests or preferences (including purchase history and marketing preferences); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).

   ii. Any individual accessing and/or using the Software through the Controller's account (**Users**) and whose information is stored on or collected via the Software.

f) The Processor can demonstrate and provide sufficient guarantees on a confidential basis as to the implementation of appropriate technical and organisational measures taken to ensure data security and protection including;

   i. Continued adherence to best practices relating to data security as described in the Boxphish Information Security Policy; and

   II. The obligations and rights of the Controller and Processor are set out in clause 3 of this DPA

SCHEDULE 2

Sub-Processors

SUB-PROCESSOR NAME	**PURPOSE OF PROCESSING**	**TYPE OF DATA PROCESSED**
AWS	*Hosted Services*	*Infrastructure*
Fresh Desk	*Technical Support*	*Customer information*
HubSpot	*Marketing*	*Customer information*
AWS	*Simple Email Service*	*Basic user information*
Salesforce	*Customer management*	*Customer information*