Cloud Design Box: Data Processing Agreement (UK)

DATA PROCESSING AGREEMENT

BETWEEN:

(the "**Data Controller**"),

AND

Cloud Design Box Ltd, a company registered in England No 09655303, having its registered office at C4DI@theDock, 31-38 Queen Street, Hull, East Yorkshire, HU1 1UU (the "**Data Processor**").

HEREBY AGREE AS FOLLOWS:

Contents

Definitions, Scope, and Roles of the Parties 3

Confidentiality 5

Data Processor Personnel 6

Security 6

Compliance documentation and audits 8

Transfer of Personal Data to Third Countries 9

Personal data breach notification 10

Sub-Processors 11

Returning or destruction of personal data 12

Data Subject Rights 13

Assistance to the Data Controller 13

Cooperation with supervisory authorities 14

Liability and indemnity 14

Miscellaneous 15

Signatures (please complete) 16

Schedule 1: Contact information (please complete) 17

Schedule 2: Personal data 18

Schedule 3: Processing personnel 21

Schedule 4: Transfers to countries outside the UK or EU 25

Schedule 5: List of current Sub-Processors 26

Appendix A: Applicable legislation 27

Definitions, Scope, and Roles of the Parties

Definitions

1. This Data Processing Agreement (**"DPA"**) and the license agreement or other written agreement between the Data Controller and the Data Processor (collectively, the "**Agreements**") reflect the Parties' agreement with regard to the Processing of Personal Data pursuant to the licence of software products, associated support, access to subscription services and/or provision of professional services to the Data Controller by the Data Processor (collectively, the **"Services"**);

2. **"UK Data Protection Law"** means all laws and regulations of the United Kingdom applicable to the Processing of Personal Data, including the UK GDPR and the Data Protection Act 2018, as defined in **Appendix A**;

3. **"EU Data Protection Law"** means all laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom applicable to the Processing of Personal Data under the Agreements including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**");

4. **"Processing"**, **"Personal Data"**, **"Data Controller"**, **"Data Processor**", "**Sub-Processor**", "**Personal Data Breach**", "**Data Protection Impact Assessment**", "**Data Subject**", "**Data Subject Rights**", "**Third Countries**" and "**Supervisory Authority**"' have the meaning ascribed to them in **UK Data Protection Law**.

Scope

1. This Data Processing Agreement applies to the Processing of Personal Data set out in Agreements executed by the parties insofar as the Processing is subject to **UK Data Protection Law**;

2. The duration of the Processing shall be the duration of the Agreements unless otherwise agreed in writing;

3. Subject matter, nature and purpose of the Processing, the categories of Personal Data, the types of Data Subjects, and purposes for which the Personal Data are being processed are those set out in the Agreements and/or Schedule 2.

Roles of the Parties

1. The Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor;

2. The Data Processor may exercise its own discretion in the selection and use of such technical means as it considers necessary to pursue those purposes, subject to the requirements of this Data Processing Agreement;

3. The Data Processor must process the Personal Data only in accordance with the Data Controller's written instructions in such manner as — and to the extent that – is appropriate for the provision of the Services, except as required to comply with a legal obligation to which the Data Processor is subject; in such a case, the Data Processor must inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

4. The Data Controller must ensure its instructions comply with **UK Data Protection Law**;

5. The Data Processor must immediately inform the Data Controller if, in its opinion, an instruction infringes **UK Data Protection Law**;

6. The Data Controller warrants that it has all necessary rights to provide the Personal Data to the Data Processor for the Processing to be performed in relation to the Services;

7. To the extent required by **UK Data Protection Law**, the Data Controller is responsible for ensuring that any necessary Data Subject consents to the Processing are obtained, and for ensuring that a record of such consents is maintained;

8. Should consent to the Processing be revoked by the Data Subject, the Data Controller is responsible for communicating the fact of such revocation to the Data Processor.

Confidentiality

1. Without prejudice to any existing contractual arrangements between the Parties, the Data Processor must treat all Personal Data as strictly confidential;

2. The obligations of confidentiality will apply during the term of this Agreement and will survive indefinitely upon termination of this Agreement.

Data Processor Personnel

1. The Data Processor must make Personal Data available only to those personnel performing Services in accordance with the Agreements;

2. The Data Processor must take commercially reasonably steps to ensure the reliability of any personnel engaged in the Processing or Personal Data;

3. The Data Processor must ensure that all personnel engaged in the Processing of Personal Data have:

    a. been informed of the confidential nature of the Personal Data;

    b. received appropriate training on their responsibilities;

    c. signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality. The obligation to treat Personal Data pursuant to such confidentiality obligations must survive the termination of the engagement of those personnel.

Security

1. The Data Processor must implement appropriate technical and organisational measures to ensure a level of security of the processing of Personal Data appropriate to the risk. These measures will include as appropriate:

    a. the pseudonymisation and encryption of personal data;

    b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

    c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

    d. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the

processing of Personal Data;

e. measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Data Controller;

f. the measures agreed upon by the Parties in Schedule 3.

2. The Data Processor will at all times have in place an appropriate written security policy with respect to the processing of Personal Data.

Ongoing Improvements to security

1. The Parties acknowledge that security requirements are constantly changing, and that effective security requires frequent evaluation and regular improvements of outdated security measures;

2. The Data Processor will therefore evaluate the measures as implemented in accordance with **Article 6** on an ongoing basis and will tighten, supplement and improve these measures in order to maintain compliance with the requirements set out in **Article 6**;

3. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in applicable data protection law or by data protection authorities of competent jurisdiction;

4. Where an amendment to the Service Agreement is necessary in order to execute a Data Controller instruction to the Data Processor to improve security measures as may be required by changes in applicable data protection law from time to time, the Parties shall negotiate an amendment to the Service Agreement in good faith.

Compliance documentation and audits

1. The Data Controller and the Data Processor will maintain records of Processing Activities. Parties shall cooperate to fulfil the obligation to maintain such records. Any material change made by a Party shall be notified to the other Party without undue delay. Each Party shall bear its own costs for its own records of Processing Activities;

2. At the request of the Data Controller, the Data Processor must make available all relevant information necessary to demonstrate compliance with **UK Data Protection Law** and shall allow for and contribute to audits, including inspections, by the Data Controller (or an independent, third-party auditor appointed by the Data Controller) in relation to the Processing of Personal Data;

3. Any audit shall be carried out on reasonable prior written notice of no less than 30 days and shall not be carried out more than once a year;

4. The Data Processor will cooperate with such audits carried out by or on behalf of the Data Controller and must grant the Data Controller´s auditors reasonable access to any premises and devices involved with the Processing of Personal Data under the Agreements;

5. The Data Processor will provide the Data Controller and/or the Data Controller´s auditors with access to any information relating to the Processing of the Personal Data as may be reasonably required by the Data Controller to ascertain the Data Processor´s compliance with this Data Processing Agreement;

6. Third-party auditors appointed by the Data Controller must be independent and must not be competitors of the Data Processor.

Transfer of Personal Data to Third Countries

1. The Data Processor must immediately notify the Data Controller of any permanent or temporary **transfers of Personal Data to a country outside of the European Economic Area** without an adequate level of protection within the meaning of **UK Data Protection Laws**;

2. The Data Processor must only perform such a transfer after obtaining written authorisation from the Data Controller, which may be refused at its own discretion;

3. Schedule 4 provides a list of transfers for which the Data Controller grants its consent upon the conclusion of this Data Processing Agreement;

4. To the extent that the Data Controller or the Data Processor are relying on a specific statutory mechanism to normalise international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid; the Data Controller and the Data Processor agree to co-operate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

Personal data breach notification

1. The Data Processor must notify the Data Controller without undue delay after becoming aware of any breach of security and/or confidentiality leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or being about to take place;

2. Any notifications made to the Data Controller shall be addressed to the employee of the Data Controller whose contact details are provided in Schedule 1 of this Data Processing Agreement, and shall contain:

    a. a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

    b. the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained;

    c. a description of the likely consequences of the incident; and

    d. a description of the measures taken or proposed to be taken by the Data Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

3. The Data Processor must make reasonable efforts to identify the causes of such a breach and must take necessary and reasonable steps in order to remediate the cause the breach;

4. Upon the Data Controller's request, the Data Processor shall provide the Data Controller with reasonable co-operation and assistance to fulfil the Data Controller's obligation under GDPR to notify a Personal Data Breach to the Supervisory Authority and to communicate on a Personal Data Breach to the Data Subject. Provided the Personal Data Breach is not due to the Data Processor's breach of its obligations under this DPA, the Data Controller will be responsible for any cost arising from the Data Processor's provision of such assistance.

Sub-Processors

1. The Data Processor must not subcontract any of its Service related activities consisting of the Processing of the Personal Data or requiring Personal Data to be processed by any third party without the prior written authorisation of the Data Controller;

2. The Data Controller authorises the Data Processor to engage the Sub Processors in Schedule 5 for the Service related activities specified and as described in **Schedule 2**;

3. Data Processor shall inform the Data Controller of any addition or replacement of such Sub-Processors giving the Data Controller an opportunity to object to such changes;

4. The Data Processor must:

    a. ensure that the Sub-Processor is bound under a written contract by the same data protection obligations of the Data Processor under this Data Processing Agreement; and

    b. impose on its Sub-Processors under a written contract the obligation to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of **UK Data Protection Law**; and

    c. supervise the Sub-Processor's compliance thereof.

5. The Data Processor shall be liable for the performance of its Sub-Processors to the same extent it would be liable if performing the Services of each Sub-Processor directly;

6. To ensure compliance with the obligations imposed on the Data Processor by this Agreement, the Data Controller may request that the Data Processor:

    a. audit a Third Party Sub-Processor; or

    b. provide confirmation that such an audit has occurred; or

    c. obtain (or assist the Data Controller in obtaining) a third-party audit report concerning the Sub-Processor's operations. The Data Controller will be responsible for any cost of third-party audit reports.

Returning or destruction of personal data

1. Upon the Data Controller's written request made within thirty days after the effective date of termination of the Agreements, the Data Processor shall, at the discretion of the Data Controller, either delete, destroy or return all Personal Data to the Data Controller and destroy or return any existing copies stored in its environment. After such a 30-day period, the Data Processor will have no obligation to maintain or provide any Personal Data and will thereafter delete Data Controller data from the services unless legally prohibited;

2. The Data Processor must notify all Sub-Processors of the Personal Data of the termination of the Data Processing Agreement and must ensure that all Sub-Processors either destroy the Personal Data or return the Personal Data to the Data Controller, at the discretion of the Data Controller.

Data Subject Rights

1. The Data Processor must, to the extent legally permitted, promptly notify the Data Controller if it receives a request from a Data Subject to exercise any of the Data Subject's Rights under **UK GDPR**;

2. Taking in account the nature of the Processing, the Data Processor must assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's Rights under the **UK GDPR**;

3. To the extent the Data Controller, in its use of the Services, does not have the ability to address a Data Subject request, the Data Processor shall, upon the Data Controller's request, provide commercially reasonable efforts to assist the Data Controller in responding to such requests, to the extent the Data Processor is legally permitted to do so and the response to such Data Subject request is required under **UK Data Protection Law**. The Data Controller will be responsible for any cost arising from the Data Processor's provision of such assistance;

Assistance to the Data Controller

1. Upon the Data Controller's request, the Data Processor shall provide the Data Controller with reasonable cooperation and assistance needed to fulfil the Data Controller's obligations under the GDPR to carry out a Data Protection Impact Assessment related to the Services to the extent the Data Controller does not otherwise have access to the relevant information, and to the extent such information is available to the Data Processor. The Data Controller will be responsible for any cost arising from the Data Processor's provision of such assistance.

2. Upon the Data Controller's request, the Data Processor shall provide the Data Controller with reasonable cooperation and assistance needed to fulfil the Data Controller's obligations under the GDPR to implement and maintain appropriate organisational and technical measures insofar as this relates to the Data Processor's Services in scope of this DPA. The Data Controller will be responsible for any cost arising from the Data Processor's provision of such assistance.

Cooperation with supervisory authorities

1. The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to prior consultations with supervisory authorities required under **Article 36 of the UK GDPR** taking into account the nature of processing and the information available to the Data Processor. The Data Controller will be responsible for any cost arising from the Data Processor's provision of such assistance;

2. The Data Controller and the Data Processor will cooperate with competent Supervisory Authorities as required by the UK GDPR. The UK's supervisory authority is the **Information Commissioner's Office (ICO)**;

3. If a party is subject to investigative or corrective powers of a Supervisory Authority, this Party must inform the other Party without undue delay, insofar as it relates to the data Processing covered by this DPA;

4. Parties shall provide reasonable assistance to each other to fulfil the obligation to cooperate with Supervisory Authorities. Each Party is responsible for its own costs arising from the provision of such assistance.

Liability and indemnity

1. The Data Processor indemnifies the Data Controller and holds the Data Controller harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Controller and arising directly or indirectly out of or in connection with a breach of this Data Processing Agreement and/or the Applicable Data Protection Law by the Data Processor;

2. The Data Controller indemnifies the Data Processor and holds the Data Process harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Processor and arising directly or indirectly out of or in connection with a breach of this Data Processing Agreement and/or the Applicable Data Law by the Data Controller.

Miscellaneous

1. In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the Service Agreement, the provisions of this Data Processing Agreement shall prevail;

2. In the event that any of the provisions of this Agreement are held to be invalid or unenforceable in whole or in part, all other provisions will nevertheless continue to be valid and enforceable with the invalid or unenforceable parts severed from the remainder of this Agreement;

3. This Agreement will be governed by and construed in accordance with the laws of England.

Signatures (please complete)

Signed	Signed
for and on behalf of the **Data Controller**	for and on behalf of the **Data Processor**
Name:	**Name:** Tony Phillips
Title:	**Title:** Chief Executive Officer
Date:	**Date:**

Schedule 1: Contact information (please complete)

Contact information of the data protection officer/compliance officer of the **Data Controller**:

Contact information of the Data Protection Officer of the **Data Processor**:

Steve Baines, Data Protection Officer, Cloud Design Box

C4DI @The Dock, 31-38 Queen Street, Hull, HU1 1UU

Tel: +44 01482 688890

Email: dataprotection@clouddesignbox.co.uk

Schedule 2: Personal data

The following table shows personal data that will be processed in the scope of the Service Agreement, and the purposes for which this data will be processed:

Subject matter of the processing	To enable Cloud Design Box to provision Office 365 student, staff and class areas including: 1. Assisting the Customer in managing resource areas for classes; 2. Accessing Personal Data in relation to the provision of the Services; Application and implementation of security measures and controls; and 3. Analysis, monitoring and reporting in relation to the Services.
Duration of the processing	Duration of the Agreements.
Nature and purposes of the processing	The provision of automated tools to pull information through from the school's MIS to setup and manage resource and collaboration areas for classes. Export of the data from Office 365 to Cloud Design Box cloud reporting service for the provision of analytics available in Office 365.
Type of Personal Data	**Contact Information** Email Address, Personal Email Address**, Phone**^

	Employment/Contract Information Job Title**, Permanent/Temporary Role**^, Start Date^, End Date^ **Government Identifiers** National Insurance No*, UPN* **Personal Identification** Forename, Surname, Admission Status^, Middle Names, Admission Number**, MIS Specific Identifiers**, Staff Code ** **User Account Information** Username, ObjectId** and Email **Class Information** Subject Codes, Class Codes, Class Enrolment, Year, House, Registration Group, Joining Date^, Leaving Date^, Teams Assignment Data** **Special categories** Photos**^
Categories of Data Subject	Staff Pupils Parents^ Guardians or student contacts^ Pre-admission students** Pre-contract staff**

	Leavers (staff and students)**

*Government identifiers are only required for some multi-tenant schools to identify users in multiple schools. These values are encrypted so they cannot be viewed by Cloud Design Box.

**Data is only processed if specified by the school, or if a feature is requested that requires this data.

^Third-Party SDS integration does not require us to process this field.

Schedule 3: Processing personnel

All staff and subcontractors have enhanced DBS checks.

Domain	Practices
Governance	**Governance Ownership** Cloud Design Box has appointed one or more officers responsible for coordinating and monitoring the security rules and procedures. **Governance Roles and Responsibilities** Cloud Design Box personnel with access to Customer Data are subject to confidentiality obligations. **Risk Management Program** Roles and risk management is done with our independent data protection officer.
Asset Management	**Asset Inventory** Cloud Design Box maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Cloud Design Box personnel authorised in writing to have such access. **Asset Handling** Cloud Design Box classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. Cloud Design Box does not allow printing of Customer Data. Cloud Design Box personnel must obtain management authorisation prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside our facilities.

Human Resources Security	**Information Governance Training** Cloud Design Box informs its personnel about relevant security procedures and their respective roles. Cloud Design Box also informs its personnel of possible consequences of breaching the security rules and procedures. Cloud Design Box will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities** Cloud Design Box limits access to facilities where information systems that process Customer Data are located to identified authorised individuals.
Communications and Operations Management	**Operational Policy** Cloud Design Box maintains information governance documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery Procedures** Cloud Design Box take backups of Salamander SharePoint configurations when accessing customer servers. Cloud Design Box have plans to restore data in the event of data loss in our analytic environment. **Malicious Software** Cloud Design Box has anti-malware controls to help avoid malicious software gaining unauthorised access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries** Cloud Design Box encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks.

	Cloud Design Box restricts access to Customer Data in media leaving its facilities. **Event Logging** Cloud Design Box logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorisation granted or denied, and relevant activity.
Access Control	**Access Policy** Cloud Design Box maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization** Cloud Design Box maintains and updates a record of personnel authorised to access Customer Data. Cloud Design Box deactivates authentication credentials that have not been used for a period of time not to exceed six months. Cloud Design Box identifies those personnel who may grant, alter or cancel authorised access to data and resources. **Least Privilege** Technical support personnel are only permitted to have access to Customer Data when needed. Cloud Design Box restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** Cloud Design Box instructs Cloud Design Box personnel to disable administrative sessions when leaving premises, or when computers are otherwise left unattended.

	Network Design Cloud Design Box has safeguards in place to ensure that individuals cannot access Customer Data beyond their assigned permissions. These controls prevent unauthorized access by ensuring that users only have access to data they are explicitly authorised to view or manage.
Information Security Incident Management	**Incident Response Process** Cloud Design Box maintains a Personal Data Breach process including, roles and responsibilities and requirements for recording of security breaches.
Technical Controls	We work with user data in Microsoft 365 via two Microsoft APIs over SSL: Microsoft Graph API (https://developer.microsoft.com/en-us/graph) SharePoint CSOM API (https://docs.microsoft.com/en-us/sharepoint/dev/sp-add-ins/sharepoint-net-server-csom-jsom-and-rest-api-index) In order to prevent credentials being visible on an engineer's machine when using the Azure browser tools, we have enabled an additional layer of encryption which encrypts specific sensitive fields. This uses the Azure Storage Client Library for .NET to encrypt these fields using 256bit AES encryption (https://docs.microsoft.com/en-us/azure/storage/common/storage-client-side-encryption).
Business Continuity Management	Cloud Design Box maintains procedures for recovering data including rerunning workloads to restore assignment analytics if the data is lost or corrupted.

Schedule 4: Transfers to countries outside the UK or EU

This schedule describes transfers to countries outside of the UK or EU — without a suitable level of protection — for which the Data Controller has granted its authorisation.

UK based Data Controllers:

NONE

Non UK Based Data Controllers:

Categories of Data Subject	Categories of data	Processing operations	Recipient Name	Recipient Location	Transfer Mechanism
All	All	All	Microsoft Azure	Regional Server based on Data Controller location e.g. UAE	EU Standard Contractual Clauses and Microsoft's Binding Corporate Rues
All	All	All	Microsoft Office 365	Regional Server based on Data Controller location e.g. UAE	EU Standard Contractual Clauses and Microsoft's Binding Corporate Rules

Schedule 5: List of current Sub-Processors

Sub-Processor	Processing Operations	Sub-Processor HQ Location	Processing Location	Service Provided	Service Criticality
Microsoft Azure	Storage, Deletion, Collection, Recording, Alteration, Restriction of all personal data in Silver, Gold and Salamander SharePoint applications.	United States	UK	Information and Communications Technology, Information Technology Services (Cloud Servers) for the Cloud Reporting Service.	Critical
SalamanderSoft	Collection, recording, storage, deletion, alteration, use of all personal data related to the Services	UK	UK or customer location (if outside the UK)	MIS data extraction and Office 365 provisioning	High
Independent Developer Contractors	Deletion, Recording, Alteration of records in Azure provisioning in response to incidents only.	UK	UK	Development of cloud infrastructure and assistance with support incidents.	Medium

Appendix A: Applicable legislation

This agreement refers to Cloud Design Box's obligations with respect to, but not exclusively limited to, the following UK and EU Data Protection Legislation.

The United Kingdom is now following the UK GDPR, which is derived from the EU GDPR. UK GDPR works in conjunction with the Data Protection Act 2018, which provides additional provisions and clarifications specific to the UK.

United Kingdom

- Data Protection Act 2018;
- UK General Data Protection Regulation (UK GDPR);
- The Privacy and Electronic Communications Regulations (PECR).

European Union

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC 'General Data Protection Regulation (GDPR).

Version Control

Version	Date	Modified By	Approved By	Version Notes
1.0	25/05/2018	Michael Curran	Michael Curran	First Version
2.0	19/02/2020	Tony Phillips	Michael Curran	Sections removed and text updated
2.1	09/03/2020	Tony Phillips	Michael Curran	Final updates to appendix
2.2	08/01/2021	Tony Phillips	Michael Curran	Updated data processing information to be clearer
3.0	13/12/2021	Tony Phillips	Michael Curran	Added student contacts for processing of student contacts
3.1	27/03/2024	Tony Phillips	Michael Curran	Updated company address. Added clarification on what data we process if there is a third party SDS provider.
4.0	28/08/2024	Darren Hemming	Michael Curran 28/11/2024	CDB branding applied. Updated for UK GDPR.
4.1	03/10/2025	Darren Hemming	Darren Hemming 03/10/2025	Contact details for DPO updated.