TA CPD HUB

GDPR & Security Due-Diligence Pack

For schools, academies and multi-academy trusts

Read alongside: Terms and Conditions • Privacy Policy • Cookie Policy • Right to be Forgotten • Data Processing Agreement

Document status: ISSUED – version 1.4
Prepared by Try This Teaching Limited with Anchorline Systems from the current TA CPD Hub configuration, hosting and email set-up and current supplier documentation. For school and Trust procurement, data protection and software request forms.

Item	Current position
Service	TA CPD Hub – online CPD platform for Teaching Assistants
Service provider / processor	Try This Teaching Limited (company no. 15392615)
Technical provider	Anchorline Systems (Chris Morris) – website development, hosting, server administration and technical support
Core hosting	Hostinger – managed by Anchorline Systems; server in the United Kingdom; backups in Germany (EU)
Primary privacy contact	info@trythisteaching.com
Pack version	Version 1.4 – 23 November 2026

This pack describes how the TA CPD Hub handles school and Trust staff data. Quick answers to the questions most often asked on school software request and data protection forms are on the next page. The Data Processing Agreement in section 15 forms Schedule 1 to the TA CPD Hub Terms and Conditions and can also be signed separately. Questions: info@trythisteaching.com.

Quick answers for school software and data protection forms

These answers cover the questions schools and Trusts most often ask when approving the TA CPD Hub. The sections that follow give the detail.

Question	Answer
Who uses the Hub? Is pupil data involved?	Adult school staff only (Teaching Assistants, support staff and their leaders). There are no pupil accounts and no pupil data is needed or requested. Staff are told not to enter pupil-identifiable information in free-text areas.
Where does the personal data come from? Is there a link to Bromcom or another MIS?	Data is entered manually. A School Lead or School Admin invites staff by email or shares the school's registration link and each member of staff completes their own account; alternatively Try This Teaching uploads a staff list (name, work email, school) supplied by the school. The Hub has no connection to Bromcom, SIMS, Arbor or any other MIS and does not import data from school systems.
What personal data is held?	Name, work email, username, job role, school/Trust, account status, assigned courses and Learning Pathways, learning progress, quiz results, certificates, webinar viewing and attendance, Skills Audit self-ratings and priorities, Reflection Journal and Community posts the user chooses to write, billing contact details for the purchasing organisation, and technical/security logs. See section 3.
Does it use biometric data (fingerprints, facial recognition, photo ID)?	No. No biometric data is collected or processed and photographs are not used for identification. Photos are not requested at all: profile and Community avatars are generated from the user's initials.
How is the system protected from unauthorised access? Password? MFA?	Every user has their own password-protected account (passwords are stored hashed and are never visible to staff or administrators) and the whole site runs over HTTPS. Access is role-based: staff see only their own learning; School Leads/Admins see only their own school; Trust Leads see only their Trust's schools. Two-factor authentication is required on all administrator accounts. The site is protected by the Wordfence firewall and login security (brute-force protection and lockouts). See section 5.
Where is the data stored?	On a managed server in the United Kingdom (Hostinger), with daily backups stored in Germany (EU). See section 4 for suppliers that may process limited data elsewhere.
Are payment card details stored?	No. Card payments are taken by Stripe (PCI DSS Level 1); card numbers never reach or are stored on the Hub.
Common Sense Media privacy rating?	Not applicable. Common Sense Media's privacy ratings assess apps and services used by children and students. The TA CPD Hub is a professional development service for adult staff with no pupil accounts or pupil data, so it has not been submitted for or rated by Common Sense Media. This pack, the Data Processing Agreement and the Privacy Policy set out how staff data is handled instead.
Is there a Data Processing Agreement?	Yes. The school or Trust is the data controller and Try This Teaching Limited is the processor. The Article 28 UK GDPR Data Processing Agreement is Schedule 1 to the Terms and Conditions, is accepted at checkout, and can be signed separately (section 15).
What happens to the data when the subscription ends?	Access is removed. Data can be exported on request and is then deleted or anonymised in line with the retention schedule in section 10, or as the school or Trust instructs.
Who do we contact?	Amjad Ali, Try This Teaching Limited – info@trythisteaching.com

1. Executive summary

TA CPD Hub is a WordPress-based professional development platform used by individual users, schools and Trusts. For school/Trust staff data, the school or Trust acts as data controller and Try This Teaching acts as data processor for delivery of the Hub service. The subscription Terms and Conditions state this controller/processor relationship and the Article 28 Data Processing Agreement (section 15) forms part of those Terms for school and Trust customers.

- Core website and database hosting is on Hostinger, managed by Anchorline Systems (server in the United Kingdom; daily backups stored in Germany, EU).
- The Hub stores user account, school/Trust, learning progress, Learning Pathway, Skills Audit, webinar viewing, quiz, completion and related administration data in the WordPress database. Staff data is entered manually or uploaded from a list supplied by the school; there is no MIS integration and no biometric data.
- WooCommerce stores customer/order information such as name, organisation, address, email, telephone, order details and transaction metadata. Raw card numbers, expiry dates and CVC are not stored by the Hub.
- Payments are processed through Stripe and supported Stripe payment methods.
- Website email is currently sent through Brevo using the FluentSMTP plugin over an encrypted connection. If the email set-up changes, this pack will be updated.
- Google Analytics is connected via Google Site Kit and should remain subject to the site's consent/cookie controls.
- Zoom is used by link for live sessions; the Hub does not intentionally upload the Hub user database to Zoom.
- No pupil personal data is required for use of the Hub and users should not enter pupil-identifiable or special-category data into reflection or notes fields. The public compliance documents are named Terms and Conditions, Privacy Policy, Cookie Policy and Right to be Forgotten.

Encryption at rest
Hostinger takes automatic daily backups of the website. Hostinger's Trust Center (trust.hostinger.com) states that databases holding personal information are encrypted at rest, at the database or disk layer where possible, and that backups are also encrypted.

2. Roles and processing relationship

Party	Role	Responsibilities
School / academy / MAT	Controller	Determines why staff personal data is used; supplies or authorises staff accounts; provides privacy information; handles lawful basis and internal governance.
Try This Teaching	Processor for school staff Hub data	Provides the TA CPD Hub; processes staff data to deliver accounts, learning, reporting, communications and support on the controller's instructions.
Anchorline Systems (Chris Morris)	Technical subprocessor / support and hosting provider	Website, server and WordPress administration; hosting management; technical maintenance; troubleshooting and development.
Hostinger	Hosting subprocessor (engaged by Anchorline Systems)	Server/hosting infrastructure and backup storage.

Important: Try This Teaching may act as an independent controller for its own business records, billing, legal compliance and direct customer relationship data. The school remains controller for staff data supplied for institutional Hub use.

3. Personal data processed

Data category	Examples	Purpose
Identity and account	Name, username, work email, job/role, account status	Account creation, login, access control and support

Data category	Examples	Purpose
Organisation	School/Trust, team membership, School Lead/School Admin role, seat allocation	Institutional access, management and reporting
Learning activity	Course/module allocation, Learning Pathway assignments, due dates and completion, video and webinar viewing progress, webinar attendance confirmations, quiz attempts/scores, completion dates/times, learning time, certificates	Deliver CPD and provide learner/manager analytics
Skills Audit and user-written content	Skills Audit self-ratings and chosen priorities; Reflection Journal entries, Community posts and member notes where used	Personalised CPD recommendations, reflection, Community discussion and manager support
Technical/security	IP address, login/activity records, browser/device, security/firewall logs and records of automatic service emails sent	Security, troubleshooting, fraud prevention and service operation
Order/billing contact	Name, organisation, billing/shipping address, email, phone, order/product, package/seat allowance, order status, payment method metadata	Subscription/order administration, invoicing and accounting
Analytics/cookies	Page views, session/device/browser and cookie identifiers where consent permits	Website usage analytics and service improvement

Special-category and pupil data: The Hub is not designed to require pupil personal data or special-category data. Schools should instruct users not to enter identifiable pupil information, safeguarding details, health information or other special-category data into free-text areas unless a separate lawful basis and processing arrangement has been agreed.

4. Hosting, location and international transfers

Area	Current position
Core platform hosting	Hostinger. The production server is located in the United Kingdom (Hostinger, Europe – United Kingdom). Hostinger stores the automatic backups in Germany (EU); the UK recognises the EU/EEA as adequate, so this is not a restricted transfer. Hostinger's Data Processing Addendum provides Standard Contractual Clauses and the UK International Data Transfer Addendum where support or group processing involves a restricted transfer.
Brevo	Transactional website email is sent through Brevo using the FluentSMTP plugin. Brevo is an EU-based (France) provider whose processor terms form part of its Terms and Conditions.
Stripe	Payment and billing data may be processed internationally. Stripe's DPA includes transfer mechanisms including the UK International Data Transfer Addendum and Stripe participates in the UK Extension to the EU-US Data Privacy Framework.
Google Analytics	Google Analytics may process website usage information internationally under Google's applicable Data Processing Terms.
Zoom	No routine database transfer is intended. If a user follows a Zoom meeting link, the user supplies information to Zoom and Zoom processes that attendance under its own terms.

Core data residency statement: The primary Hub server/database is hosted by Hostinger in the United Kingdom, with backups stored in Germany (EU). It would not be accurate to state that no personal data ever leaves the UK because hosting support, email, payment and analytics providers may process limited data internationally.

5. Security statement

Control	Current position / assurance
Encryption in transit	The public website is served over HTTPS/TLS. Transactional email is passed to Brevo over an encrypted connection.
Encryption at rest	Hostinger's Trust Center states that databases holding personal information are encrypted at rest, at the database application or disk layer where possible, and that backups are encrypted using the backup manufacturer's technology.
Application access controls	Individual accounts with role-based access: staff see only their own learning; School Leads/Admins see only their own school's staff and analytics; Trust Leads see only their Trust's schools; site administration is limited to Try This Teaching and Anchorline Systems. Hub access is tied to active membership/team status.
Administrative access	Restricted to authorised Try This Teaching and Anchorline Systems personnel. Amjad Ali has administrative access; Anchorline Systems (Chris Morris) provides hosting and technical administration.
Passwords	Every user has an individual password-protected account. Passwords are stored hashed by WordPress and are never visible to staff or administrators; resets are by emailed link. Two-factor authentication (authenticator app) is required on all administrator accounts through Wordfence Login Security.
Network/security layer	Wordfence web application firewall and login security (brute-force protection, lockouts and alerts) on the site; hosting-level security controls provided by Hostinger. Configuration and security settings are maintained by Anchorline Systems.
Software maintenance	WordPress, plugin and Hub code maintenance is undertaken by Anchorline Systems. Security/vulnerability management includes updates, incident investigation and technical remediation.
Payment security	Raw payment-card details are handled by Stripe's payment components and are not stored in the Hub database. The Hub retains order and billing/contact records.

6. Backups and disaster recovery

Backup set	Schedule	Retention
Daily	Every day (automatic, Hostinger)	Rolling daily copies kept by Hostinger, stored in Germany (EU)

Backup contents: Hostinger's automatic backups cover the website files and databases.

Backup storage: Backups are stored and managed by Hostinger in Germany (EU). Hostinger states that backups are encrypted.

Recovery: Files and databases can be restored from the Hostinger control panel (hPanel) by Anchorline Systems.

Restore testing
Anchorline Systems carries out and records a test restore from backup at least annually.

7. Payments and e-commerce

WooCommerce records retained by the Hub include customer and order information such as name, organisation, billing/shipping address, email, phone, order/product details, selected package/TA allowance, transaction status and the payment method used.

- Stripe is the payment processor for card and supported payment methods, including supported wallets and Bacs Direct Debit where enabled.
- Raw card number, expiry date and CVC are not intended to be stored in the WordPress/WooCommerce database.
- Stripe is a PCI DSS Level 1 service provider and maintains its own DPA and transfer safeguards.
- Try This Teaching remains responsible for its own merchant PCI obligations appropriate to the Stripe/WooCommerce integration used.

8. Email, analytics and webinar services

Service	Use on the Hub	Data involved
Brevo (via FluentSMTP)	Transactional website email (account, password, order, notification and campaign emails)	Recipient name/email, message content and mail-routing metadata
Google Analytics via Site Kit	Website usage analytics	Page/session/device/browser and cookie/identifier data where consent permits
LearnDash	Self-hosted LMS functionality inside WordPress	Learning, quiz, completion and course progress stored on the Hub database; not treated here as an external analytics processor
Zoom	Live webinar links	No automatic Hub database upload is intended. A user who joins Zoom supplies attendance/account/device data directly to Zoom.

9. Subprocessors and external services register

Provider	Purpose	Location / transfer position	Safeguard / notes
Anchorline Systems (Chris Morris)	Technical administration, development, support and hosting management	UK-based operational support	Authorised access only; covered by written processor terms with Try This Teaching (Website Support Agreement).
Hostinger (Hostinger International Ltd / Hostinger UK Limited)	Hosting and backup infrastructure	Server in the United Kingdom; backups in Germany (EU); some support/group processing may occur outside the UK/EEA	Hostinger Data Processing Addendum (SCCs and UK International Data Transfer Addendum); ISO/IEC 27001 certified.
Brevo	Transactional email (via FluentSMTP)	EU-based provider (France); limited international processing possible	Brevo processor terms appended to its Terms and Conditions; published GDPR compliance documentation.
Stripe	Payments and billing processing	International processing possible	Stripe DPA; UK Addendum/other transfer mechanisms; PCI DSS Level 1.
Google	Google Analytics (via Site Kit)	International processing possible	Google Analytics/Data Processing Terms; cookie/consent controls required.

Provider	Purpose	Location / transfer position	Safeguard / notes
Zoom	Optional webinar attendance	User may be processed by Zoom when joining a meeting	Not a routine Hub database subprocessor where links only are used; Zoom privacy/DPA applies to attendance.

10. Data retention and deletion

Current position: Live access is removed when a School or Trust subscription ends. Data can be exported on request during a 30-day window and is then deleted or anonymised in line with the schedule below, unless the school or Trust instructs otherwise or continued retention is legally required. Individual deletion requests can be made through the Right to be Forgotten page or info@trythisteaching.com.

Retention schedule

Record type	Position	Status
User profile / organisational membership	Retain while the subscription is active; allow a 30-day post-termination export/request window; then delete or anonymise identifiable Hub account data within 90 days unless the Controller instructs otherwise or continued retention is lawfully required.	Standard position
Learning progress, completions, quiz results, certificates	Retain while the subscription is active and during the 30-day export/request window; then delete or anonymise identifiable learning records within 90 days unless the Controller instructs otherwise or continued retention is lawfully required.	Standard position
Reflection journal / member notes	Retain only while needed for the learning service and the short post-termination export/request period; then delete or anonymise within the same 90-day maximum unless earlier deletion is validly requested or continued retention is lawfully required.	Standard position
Orders, invoices and accounting records	Retain in accordance with UK accounting, VAT, tax and legal requirements. VAT/business records are generally kept for at least six years where applicable.	Legal requirement
Backups	Daily automatic backups are kept on Hostinger's rolling schedule. Deleted live data may persist in backup sets until they expire.	Configured
Security/server logs	Kept only for as long as needed for security monitoring and troubleshooting, then rotated or deleted automatically.	In place

11. Incident and personal data breach procedure

1. Identify and contain: Anchorline Systems/Try This Teaching isolates the affected account, site, plugin, credential or server component and preserves relevant logs/evidence.
2. Assess scope: identify affected data categories, users/controllers, likely cause, duration, access/exfiltration evidence and risk to individuals.
3. Notify Try This Teaching immediately and maintain an incident log with actions, decisions and timestamps.
4. Where school/MAT-controlled staff data is affected, notify the relevant controller without undue delay with sufficient information to support its UK GDPR assessment.
5. Support the controller with regulatory/data-subject notifications. The controller is responsible for deciding whether an ICO notification is required and, where applicable, meeting the statutory 72-hour reporting window.

6. Eradicate and recover: patch vulnerabilities, reset credentials/keys, restore clean data/services where necessary and monitor for recurrence.
7. Post-incident review: document root cause, lessons learned, control improvements and any required subprocessor notifications.

12. Data subject rights and controller assistance

Try This Teaching provides reasonable assistance to schools/MATs with requests relating to access, rectification, erasure, restriction, portability and objection where the request concerns Hub data processed on the controller's behalf.

- Account/profile data can be reviewed and corrected administratively.
- School/Trust access and memberships can be revoked or removed.
- Learning and account records can be exported or administratively deleted/anonymised where technically and legally appropriate.
- Backups are subject to normal retention rotation; deleted data may remain in backup media until expiry and should not be restored into live use except for disaster recovery.

13. Certifications and assurance

Organisation	Current assurance position
Try This Teaching	No independent ISO 27001, SOC 2 or Cyber Essentials certification is held or claimed.
Anchorline Systems	No certification is claimed in this pack. Technical controls and operational practices are described on their merits.
Hostinger	Hostinger states it holds ISO/IEC 27001 certification for its information security management system, audited by TÜV Thüringen.
Brevo	Brevo publishes GDPR compliance and security documentation.
Stripe	Stripe states it is a PCI DSS Level 1 service provider, independently assessed annually, and makes SOC reporting available.

14. Ongoing assurance

Area	Activity	Purpose
Retention	Apply the retention schedule in section 10 at the end of each subscription, or as the school or Trust instructs.	Clear end-of-contract commitments.
Documentation	Review this pack, the Data Processing Agreement and the subprocessor register at least annually and before any new subprocessor is used.	Keeps customers' records accurate.
Access security	Keep two-factor authentication enforced on all administrator accounts and review administrator access.	Reduces the risk of account compromise.
Analytics	Keep Google Analytics consent behaviour on logged-in Hub pages under review.	Consistent handling of cookies/identifiers.
Recovery	Carry out and record a test restore from backup at least annually.	Evidence that disaster recovery works.

15. Data Processing Agreement (Article 28 UK GDPR)

This Data Processing Agreement forms Schedule 1 to the TA CPD Hub Terms and Conditions for School and Trust subscriptions and is accepted at checkout. Where a school or Trust's procurement process requires a signed copy, it can be signed below and returned to info@trythisteaching.com.

Parties

Party	Details
Controller	The subscribing school, academy, federation or multi-academy trust identified in the subscription/order ("Controller").
Processor	Try This Teaching Limited (company no. 15392615), registered office 9 Ruskin Way, Woosehill, Wokingham, United Kingdom, RG41 3BP; VAT no. 460722506 ("Processor"). Contact: Amjad Ali – info@trythisteaching.com.

1. Scope and duration

This DPA applies where the Processor processes Personal Data on behalf of the Controller in connection with the TA CPD Hub. Processing continues for the duration of the Controller's subscription and any agreed post-termination return/deletion period.

2. Subject matter and purpose

The Processor will process staff Personal Data only as necessary to provide, secure, administer and support the TA CPD Hub, including account creation, learning delivery, learning analytics, school/Trust administration, communications, support and reporting.

3. Processing on documented instructions

The Processor shall process Personal Data only on the documented instructions of the Controller, including instructions contained in the subscription agreement, this DPA, support requests and authorised administrative actions, unless UK law requires otherwise.

4. Confidentiality

The Processor shall ensure that persons authorised to process Personal Data are subject to appropriate confidentiality obligations and only access data to the extent necessary for their role.

5. Security

Taking into account the nature of the processing, the Processor shall implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Current measures are described in the TA CPD Hub GDPR & Security Due-Diligence Pack and may be updated as the service evolves.

6. Subprocessors

The Controller gives general written authorisation for the Processor to use subprocessors necessary to deliver the service, subject to the Processor maintaining an up-to-date subprocessor register and imposing data-protection obligations that provide an equivalent level of protection where Article 28 requires this. The Processor remains responsible to the Controller for its subprocessors' processing within the scope of this DPA.

7. International transfers

The Processor shall not make a restricted transfer of Controller Personal Data unless an applicable UK GDPR transfer mechanism or adequacy arrangement is in place. Where relevant, supplier DPAs, SCCs, the UK Addendum and/or recognised data privacy framework mechanisms may be relied upon.

8. Data subject rights

Taking into account the nature of the processing, the Processor shall provide reasonable assistance to the Controller, insofar as possible, with requests from data subjects exercising rights under UK data protection law.

9. Security incidents and personal data breaches

The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data Breach affecting Controller Personal Data and shall provide available information reasonably required for the Controller to meet its legal obligations.

10. DPIAs and regulatory cooperation

The Processor shall provide reasonable information and assistance, taking into account the nature of processing and information available to it, where the Controller requires support with a data protection impact assessment or consultation with the Information Commissioner.

11. Return and deletion

At the end of the services, the Processor shall, at the Controller's choice and subject to applicable law, return/export relevant Controller Personal Data and delete or anonymise Personal Data that is no longer required. Data contained in backup media may remain until normal backup rotation expires and will remain protected from routine use.

12. Audit and information rights

The Processor shall make available information reasonably necessary to demonstrate compliance with Article 28 obligations and shall permit reasonable audits or inspections subject to appropriate notice, confidentiality, security and cost arrangements.

13. Controller obligations

The Controller is responsible for ensuring that it has a lawful basis for providing staff Personal Data to the Processor, that staff receive appropriate privacy information, and that instructions given to the Processor comply with applicable data protection law.

14. Liability and precedence

Nothing in this DPA relieves either party of its direct obligations under applicable data protection law. If there is a conflict between this DPA and other terms relating specifically to processing of Controller Personal Data, this DPA shall take precedence to the extent of that conflict.

Schedule A – Processing details

Item	Details
Data subjects	School/MAT employees, Teaching Assistants, school/Trust managers/admins, purchasing/account contacts and authorised Hub users.
Personal data	Name, username, work email, job/role, school/Trust affiliation, School Lead/Admin status, account/membership status, learning allocations/progress, Learning Pathway assignments and completion, webinar viewing and attendance, Skills Audit self-ratings and priorities, quiz data, completion records, learning time, certificates, reflections/notes, Community posts, records of service emails sent, support/security logs, billing/order contact data and technical identifiers. Source: entered by the Controller's authorised School/Trust Lead or School Admin, by the staff member, or uploaded by the Processor from a list supplied by the Controller; no MIS integration.
Special-category data	Not required or requested. No biometric data, photographs for identification, pupil data or payment card numbers are processed. Users should not enter pupil-identifiable or special-category information into the Hub.
Frequency	Continuous/regular for the duration of the service.
Nature	Collection, storage, retrieval, organisation, access control, reporting, communication, export, support, deletion/anonymisation and backup.
Purpose	Provision and administration of the TA CPD Hub and associated CPD reporting/support.
Duration	Subscription term plus the retention/deletion period set out in section 10 of the TA CPD Hub GDPR & Security Pack, or as the Controller instructs.

Schedule B – Subprocessors / services

Provider	Service
Anchorline Systems (Chris Morris)	Technical administration, support, development and hosting management
Hostinger	Hosting/server and backup infrastructure (server in the United Kingdom; backups in Germany, EU)
Brevo	Transactional email sending (via FluentSMTP)
Stripe	Payment processing
Google	Google Analytics where enabled

Zoom is treated separately where the Hub provides meeting links only and a user chooses to join Zoom directly. The Processor will update this register before any new subprocessor processes Controller Personal Data.

Signature / incorporation

For the Controller	For Try This Teaching Limited
Name: _____ Role: _____ Date: _____ Signature: _____	Name: _____ Role: _____ Date: _____ Signature: _____

16. Reference sources

ICO – Contracts and liabilities between controllers and processors: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/contracts-and-liabilities-between-controllers-and-processors-multi/

ICO – What needs to be included in the contract: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/contracts-and-liabilities-between-controllers-and-processors-multi/what-needs-to-be-included-in-the-contract/

Hostinger – Data Processing Addendum: https://www.hostinger.com/uk/legal/dpa

Hostinger – ISO 27001 certification: https://www.hostinger.com/blog/iso-27001/

Hostinger – Trust Center (security controls, including encryption): https://trust.hostinger.com

Brevo – How Brevo complies with the GDPR: https://help.brevo.com/hc/en-us/articles/360001258744-How-does-Brevo-comply-with-the-GDPR

Stripe – Data Processing Agreement: https://stripe.com/gb/legal/dpa

Stripe – PCI compliance guidance: https://stripe.com/guides/pci-compliance

Google Analytics – Data Processing Terms: https://support.google.com/analytics/answer/3379636?hl=en

Zoom – Privacy and trust resources: https://www.zoom.com/en/trust/privacy/

Prepared from: Hostinger hosting and backup configuration; Wordfence configuration; FluentSMTP/Brevo email configuration; WooCommerce/Stripe checkout configuration; TA CPD Hub Terms and Privacy Policy; current Hub technical configuration supplied by Anchorline Systems.