Our Company and Product

Every day in universities across the globe, educators use PebblePad's Learning Journey Platform to help students and staff plan for their learning, record and reflect on their experiences, collate and curate evidence of achievement, and share and showcase evidence of their evolving capabilities. All of this is supported by tools for creating integrated and authentic assessment opportunities.

Founded in 2003, PebblePad – with our Head Office in the UK and a global team of now over 80 employees - has a track record of consistently delivering exceptional customer service and pedagogical support. As a company, we are a trusted global technology provider to over 100 Higher Education institutions.

At PebblePad we recognise the vital importance of the trust placed in us by our clients in relation to the security of the platform and protection of their data. We take our commitments and responsibilities seriously; data security and privacy is our highest priority.

1. Security and Risk Management Objectives

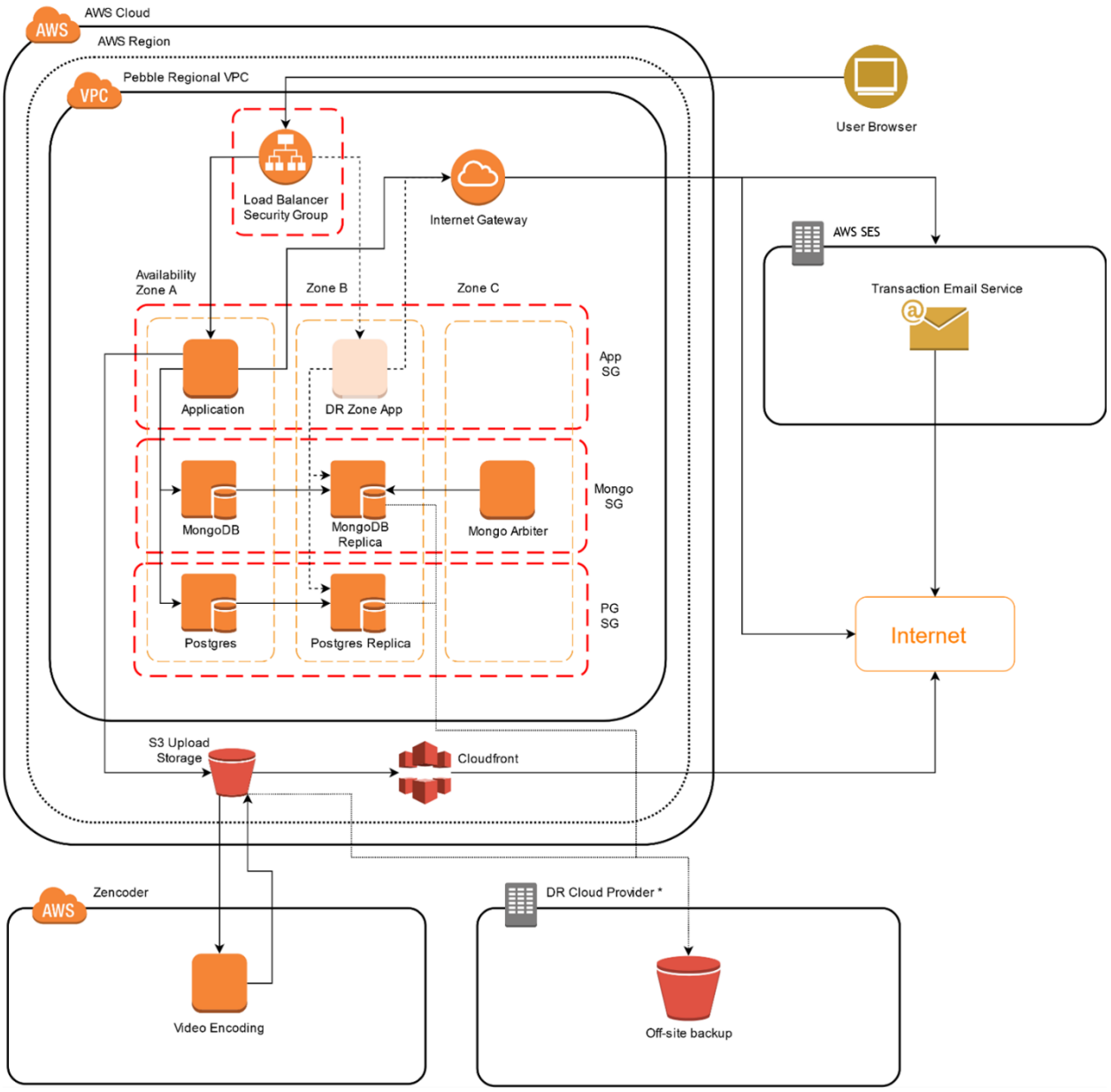
We are a Cyber Essentials, Cyber Essentials+ and ISO 27001 certified organisation. Our key security objectives include:

- Protecting the information assets that Pebble Learning Ltd handles, stores, exchanges, processes and has access to and ensure the ongoing maintenance of their confidentiality, integrity and availability.
- Ensuring the company complies with all relevant legal, customer and other third-party requirements relating to information security.
- Continually improving Pebble Learning Ltd.'s information security management system and its ability to withstand threats that could potentially compromise information security.

2. Architecture Overview

PebblePad is provided as a fully hosted and managed Software as a Service (SaaS) solution hosted in Amazon Web Services and is split into four main tiers. The database servers run on Ubuntu Linux, application servers on Windows Server. The application servers host all backend services and API endpoints involved in running PebblePad. These are .NET based and written in C#. The end user UI is a HTML5 web application written in React and AngularJS, which utilises the .NET API endpoints to access content and implement all interactions.

Storage of uploaded user content is provided by Amazon's S3 service, providing effectively unlimited storage for file uploads. Any video and audio content uploaded is transcoded to a common format to ensure compatibility across devices. Download and playback of uploaded files is provided though AWS Cloudfront to eliminate impact of video bandwidth requirements on our servers and improve throughput for users.


AWS Cloud
AWS Region
Pebble Regional VPC
VPC
User Browser
Load Balancer Security Group
Internet Gateway
AWS SES
Transaction Email Service
Availability Zone A
Zone B
Zone C
App SG
Application
DR Zone App
Mongo SG
MongoDB
MongoDB Replica
Mongo Arbiter
PG SG
Postgres
Postgres Replica
Internet
S3 Upload Storage
Cloudfront
Zencoder
Video Encoding
DR Cloud Provider *
Off-site backup

3. Policies & Processes

We are a Cyber Essentials, Cyber Essentials+ and ISO 27001 certified organisation. Our Information Security Management System (ISMS) conforms fully with the ISO 27001 standard and is the framework used for our policies and processes relating to information security. Our policies are regularly checked, reported on, improved and internally audited in-line with ISO standards. Yearly external audits independently review our working practices to confirm our ISO 27001 certified status. Policies that do not contain sensitive information relating to security can be provided upon request.

The CTO is responsible for our adherence to the Information Security Management System and our Information Security Officer is responsible for daily monitoring and ongoing review. All developers are trained in security and safe coding practices, and all staff receive information security and data protection training.

PebblePad fully complies with current data protection legislation and provides customers with access to administration tools which allow them to meet their obligations.

A copy of our privacy statement can be found at https://pebblepad.co.uk/privacy.aspx https://www.pebblepad.com.au/l/privacy.aspx

For UK and EEA customers our GDPR policy can be found at https://www.pebblepad.co.uk/l/gdpr.aspx.

4. Third Parties

Our policy is to minimize the number of third parties in use within the system. Where third parties are required, we ensure that their data security, including uptime, data protection and privacy is of an equivalent standard to our own and have binding data processing agreements incorporating GDPR model contractual clauses in place to support this.

A copy of our current sub-processors can be requested by emailing datasecurity@pebblepad.com.

5. Data Centres

All servers are cloud hosted with primary hosting provided by Amazon Web Services (AWS) and backup hosting for disaster recovery purposes by Google, Microsoft or IBM depending on your location. These solutions provide high levels of physical and network security as well as hosting provider diversity. All providers maintain an audited security program, including SOC 2 and ISO 27001 compliance, full details of which can be found at:

- https://aws.amazon.com/compliance/
- https://cloud.google.com/security/compliance/
- https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance/

These world-class server providers leverage the most advanced facilities such as power, networking, and security. Facilities uptime is guaranteed between 99.95% and 100%, and the facilities ensure a minimum of N+1 redundancy to all power, network, and HVAC services.

The data centres' physical security protections include dedicated security staff, strictly managed physical access control, and video surveillance.

Details of hosting locations can be found in region-specific sub-processor documents which can be provided upon request.

6. Data Storage

Data is hosted on Amazon Web Services with data storage provided by replicated S3, MongoDB and PostgreSQL services. Data at rest is encrypted using AES-256. In addition, a nightly encrypted backup is transferred to a separate cloud service as detailed in a region-specific sub-processor document; these backups are maintained for 6 months.

All storage media is accounted for in our Asset Management Policy and encrypted where necessary. When being repurposed or at end-of-life, the media is securely erased internally and if no longer required is professionally disposed of by an accredited company.

7. Key Management

Encryption is used to protect all confidential information including all customer data in conjunction with other technical controls such as access control. Our key management processes maintain requirements for generation, management and destruction of keys, along with determining cipher strengths, access to keys and auditing.

All keys are stored in secure key vaults with access protected and all actions logged. Key management used in the provision of customer services is through Amazon's AWS Key Management service.

8. Software Development

We use Agile development frameworks to deliver working software on an incremental basis. These frameworks specifically support planning, development and testing as continual ongoing activities to promote transparency and reduce risk. We incorporate checks throughout our development life cycle to ensure key areas such as security, performance and accessibility pass our rigorous quality assurance standards.

All development work is code reviewed and approved by senior developers; only after this process can the code be considered a release candidate. Prior to a system upgrade the release candidate is regression tested and our release management team follows a detailed process to safely deploy the update onto our production servers.

We follow secure coding guidelines drawn from multiple sources for the technologies we use (e.g. NIST, Microsoft, OWASP). Mitigation against common security vulnerabilities is designed as a core part of the application wherever possible. PebblePad includes specific protection and SQL Injection via enforced parameterization of queries, CSRF and XSS attacks through built-in .NET capabilities, and application-level filtering.

9. Quality Assurance

We operate cross-functional teams with dedicated test specialists embedded in each development team. Our test specialists are closely involved in all stages of the development lifecycle to fully understand new developments and advise developers about testing methods, different customer use cases and platform consistency.

Our test specialists work with their teams to create test scripts and then have these scripts approved by senior testers. They are responsible for in-sprint testing, automated tests and lead regression testing prior to a release. Overall responsibility for our quality assurance processes resides with our Quality Assurance Manager who works across our development teams to ensure the quality of our testing is maintained.

Customer data is never used by PebblePad in development or QA environments.

10. Product Updates

Release notes detailing new features and fixes are provided as part of the notification of each new release so our institution support contacts can disseminate this information to all relevant parties within the institution.

Customers are often asked to contribute to major PebblePad initiatives through conversations with their dedicated Client Success Managers. We also welcome participation at regional and international community events.

Major application upgrades:

- We will provide 3 months' notice of major system upgrades. Prior to a release we will share information about what we have changed or added, why we have done this, the benefit to our customers and how new feature is used.

Minor application upgrades:

- The system is upgraded regularly throughout the year to release new features and fix bugs. Usually a minimum of 1 week's notice is given prior to this release. The update is performed outside normal business hours.
- We complete all testing prior to release; if a customer wishes to also complete their own testing this is possible in our testing environment TAQAS.
- Critical fixes are performed without prior notice outside normal business hours.
- All upgrades and patches are required; however, some new features can be turned off.

PebblePad has the ability to rollback any unsuccessful system change and return to the state it was in prior to the attempted change. Roll back scenarios are included in all system upgrade work.

11. Infrastructure Maintenance and Patch Management

Regular maintenance of servers and application of OS patches occurs throughout the year, and any maintenance expected to require downtime will be notified in advance. OS patches are tested in pre-production environments prior to rollout but are expedited where appropriate to risk level.

- Regular maintenance, such as the application of OS security updates, is carried out during a nightly maintenance window of 0300-0400h. No downtime is normally associated with these updates.
- Other planned maintenance may be performed outside normal business hours, and a minimum of 7 working days' notice will be given in advance.
- If emergency maintenance is required, we will endeavour to perform this outside normal hours and provide as much notice as possible.

12. Authentication

PebblePad supports a range of authentication options which are common between student and admin users. The following options are supported:

- LTI / OAuth 1.0a
- LDAP (including Active Directory)
- SAML2 (ADFS, Shibboleth and all other compatible options)
- PebblePad internal authentication

Passwords stored locally by PebblePad's internal authentication method are hashed using PBKDF2.

For most scenarios we recommend integration with customer authentication systems via SAML2 to allow full control over password handling, including alignment with password complexity, aging and MFA requirements.

Further information on integration options can be found on our community site https://community.pebblepad.co.uk/support/solutions/articles/13000030863-pebblepad-integration-options

13. Access Controls in PebblePad

PebblePad is a multi-tenant solution by design, with separation enforced by the application at the user and customer level. All data entered into PebblePad is private by default and permissions are enforced by access control lists.

The platform provides the flexibility for a single user to have multiple permissions-based roles in different contexts e.g., student in one context, assessor in another. Further information on roles can be found here https://community.pebblepad.co.uk/support/solutions/articles/13000033785-pebblepad-administration-roles-and-permissions

14. Network Security

All network traffic for end users and systems administration is encrypted using TLS 1.2 or other encryption methods of equivalent strength.

Firewall rules can only be changed by the platform team who is responsible for the operation and security of the production versions of PebblePad. Firewall change requests are subject to our standard change management procedure.

Changes to security-related AWS configuration results in an immediate alert to the platform team. If the change is not expected, it triggers an investigation into the source of the change and is followed up with corrective actions.

15. Corporate Security

PebblePad ensures that all employment candidates are subject to background verification, appropriate to the position and within the restrictions of UK law, prior to employment. All staff are contractually obligated to adhere to our information security policy, we deliver in-depth data security and privacy training as part of our induction, and provide regular refresher training. Additionally, all staff are subject to a confidentiality clause as part of their employment contract.

PebblePad staff access to sensitive information is limited on a least privilege basis. Staff are trained in appropriate use of data, and reporting mechanisms are in place for misuse of data. Access to server management is restricted to senior systems staff from our management network using named accounts with 2 factor authentication. Privileges granted to PebblePad staff on all systems are reviewed at least once per year as part of an annual review. In addition to this, these privileges are also reviewed during any change of job role, as part of changes to operational systems and during regular audits of system access.

PebblePad's office is secured by key code locks and building access is controlled using individually assigned key cards, which are deprovisioned if lost or when no longer needed (e.g., employee termination, infrequent use, etc).

16. Disaster Recovery and Business Continuity Plan

Disaster recovery plans are in place detailing expected failure scenarios and resolutions plans depending on the type and severity of failure, including simple fail-over scenarios for single server failure and full data-centre migration for a major outage.

Customers will be notified of service outages and progress towards restoration via our standard email communication channels, and messages are also posted to Twitter.

PebblePad has an SLA guaranteeing 99.9% uptime over a rolling 12-month period which can be monitored via our status site at https://status.pebblepad.co.uk/

Our Business Continuity Plan aims to provide a flexible response so that PebblePad can respond to a disruptive incident (incident management) and maintain delivery of critical activities/services during an incident (business continuity) and return to 'business as usual' (resumption and recovery).

The following activities/services/functions are covered by our Business Continuity Plan:

- PebblePad Service Hosting
- Customer Support
- Software development
- Finance and administration
- Sales and marketing

For PebblePad service hosting, in normal failure circumstances we would recover from replica servers and the RPO is 5 minutes with an RTO of 1 hour. In the event of a total unrecoverable failure of Amazon's infrastructure in a hosting region we would fall back on nightly backups stored offsite and restore the service in a different provider. The RPO in this case is 48 hours and RTO is 8 hours.

17. Monitoring

We use Icinga to monitor all servers, services and applications for performance issues as well as faults. Our cloud platform also monitors and logs performance data.

We scale our system proactively based on trends extrapolated from these systems. PebblePad can scale horizontally and vertically to accommodate short and long-term variations in workload. Vertical scaling is supported by Amazon's EC2 service. This is generally actioned as part of an overnight maintenance period due to a brief period of downtime when restarting affected servers. Horizontal scaling is facilitated by splitting or replicating application components across additional servers in response to long term requirements

Centrally managed anti-virus and host intrusion protection is installed on all application servers, capable of detecting and blocking common network and local exploits.

Activity, security and exception logs are generated by PebblePad and the underlying servers and are regularly reviewed, including for troubleshooting purposes. Activity logs for auditing assessment actions are available within the management UI. Audit logs are retained for a minimum of a year and have appropriate protection against alteration and loss.

18. Change Management

Our Change Management Process ensures that changes undertaken to any managed systems are controlled to minimize risks to security and availability. Changes require review, testing and approval before they are made.

Emergency changes follow the same process as major changes with the same documentation requirements. If there are time constraints, they may be actioned prior to approval, but the changes must still be filed and approved after the fact.

Our application server setup process makes use of AWS-provided images as a base install and layers customisations on top of this using managed configuration scripts for the system and an automated deployment system for the application. Changes to the deployment and configuration scripts are handled via change management procedures.

19. Auditing and Incident Management

For any incident that occurs, immediate actions must be taken to limit its impact. Evidence will be obtained and preserved to enable an accurate investigation to be completed. Root causes must be identified, and corrective action taken to prevent a recurrence.

We have scheduled internal audits conducted by our Information Security Officer. Results of audits are reported within regular ISO management meetings and to our board of directors.

Applications are tested annually for vulnerabilities by a third party. We perform monthly internal vulnerability scans.

All security issues are treated as high priority and immediately investigated. If a hotfix (a small and often temporary fix) can be applied to mitigate the security risk posed it will be performed as quickly as possible, pending sign-off of all standard quality checks.

Last updated: 08/08/2022