Data protection and secure hosting policy

Data protection principles

The Development Manager is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

General provisions

1. This policy applies to all personal data processed by TDM.
2. The Responsible Person shall take responsibility for TDM's ongoing compliance with this policy.
3. This policy shall be reviewed at least annually.
4. TDM is registered with the Information Commissioner's Office as an organisation that processes and controls personal data. See our data protection policy for further details.
5. TDM's staff must read this policy in conjunction with TDM's Information Security Policies and Procedures.

Lawful purposes

1. Individuals have the right to access their personal data and any such requests made to TDM shall be dealt with in a timely manner.
2. All data processed by TDM must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
3. TDM shall note the appropriate lawful basis in the Register of Systems.
4. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
5. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in TDM's systems.

Data minimisation

1. TDM shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
2. Data will not be held on any local systems at TDM, personal data will only be used on our hosted platform (see below for more information on our hosted platforms)

Accuracy

1. TDM shall take reasonable steps to ensure personal data is accurate.
2. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving / removal

1. To ensure that personal data is kept for no longer than necessary, TDM has put in place a document retention policy – stating archiving procedures for each area in which personal data is processed and reviews this process annually.
2. The retention policy shall consider what data should/must be retained, for how long, and why.

Security

1. TDM shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
2. Access to personal data shall be limited to staff who need access and appropriate security should be in place to avoid unauthorised sharing of information.
3. When personal data is deleted this should be done safely such that the data is irrecoverable.
4. Appropriate back-up and disaster recovery solutions shall be in place.

Breach

1. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, TDM shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

Server hosting environment

1. All servers are hosted in the UK; our main cluster is in Maidenhead and backup data is stored in Gosport.
2. Our servers are utilising a VMware vSphere (ESXi) 5.5 High availability configuration which will ensure that should the server fail for any reason the service will continue to run on a backup system until the problem is resolved. Should a server experience any difficulties all services will automatically be ported to another server in the cloud and will continue to run, this entire process is completed in seconds. We expect 99.99% server uptime with this set-up.

Storage

1. TDM are utilising a Dell High Availability SAN storage device running Raid 6 over a 10 Gbit iSCSI connection, with this set-up can continue seamless access to storage in the event of failure.
2. Our server management team are on hand 24/7 and available in the extremely unlikely event of a system failure. We also have a 24/7 emergency 4-hour support with our storage vendor (Dell).
3. In additional to the localised resilience we will also take daily (or hourly, we can schedule any interval you feel would suit your needs*) backups of the system which is stored on a SAN device hosted in a different data centre but on the same network. This means that in the worst-case scenario we will still have a working copy of your system. Due to the extensive size of Moodle and Totara sites we will take an incremental backup. This means that the first backup taken will be a complete system backup and from this point onwards we will take a copy of any data that has changed.
4. Backups are stored in a day/week/month/year format which means we will always have a backup from the previous 7 days, 4 weeks and 12 months. Due to the dynamic nature of online learning it's paramount to keep this data up to date with frequent backup intervals.
5. Data recovery is a replication of the data migration in process in that we will use the latest full backup available to create a "new" instance of your platform from the backup files. This is included as part of your backup service.
6. We will schedule all minor updates to the operating system to happen automatically, this will be scheduled at off peak times to ensure performance is not impacted. This is checked and monitored through the use of internal email and reports which will arrive to our inbox daily to ensure all is well. We can forward these reports if you wish but our customers usually prefer to take care of this for you
7. For major updates we will agree a maintenance window as far in advance as possible, we're always keeping up to date with the latest LMS developments and are actively involved in the community, as well as contributing code base to further enhance the learner experience. This means we will know well in advance of any upcoming requirements to upgrade. On occasions which we are not able to foresee (such as the recent Heartbleed vulnerability) we will advise you accordingly and take immediate action (with your agreement) to remedy the situation.

8. We typically upgrade Moodle on an ad-hoc basis with different timescales for each customer. On occasions where important security fixes have been made we will advise at that time to schedule an update to the system. These minor updates do not usually involve a significant period of downtime. Major updates, such as moving Moodle/Totara/Mahara versions is a more involved process which will require the update of relevant add-ons and customisations to be fully checked. In this instance we may advise that a test update be carried out in advance. If you prefer we can agree upon a more rigid upgrade schedule, the downside of this is we may be waiting longer to apply important updates or incurring downtime to apply very minor code changes.

    For customers an hourly backup schedule may invoke extra storage and management costs and performance implications will also have to be considered.

Vendor certifications

Our hosting vendor holds ISO 27001 and 9001 accreditations.

1. **Maximum Security**

- 24 x 7 x 365 Manned Security & Monitoring
- Smart Card access policies
- Internal and External CCTV systems
- Security breach alarms

2. **Stable Environmental Conditions**

- 24 x 7 environmental monitoring systems
- Constant evaluation and testing of all systems
- N+1 redundant Heating Ventilation Air Conditioning (HVAC) system
- Fully redundant air handling units provide constant fresh airflow
- Raychem Fluid Detection
- FM200 fire suppression equipment

3. **Power**

- Dual independent power feeds, backed up by dual battery string Uninterrupted Power Supplies (UPS) systems (deployed as standard)
- 2 Megawatt diesel generators - protect services from any single power failure

4. **Interconnectivity**

- Diverse fibre routing via multiple carriers
- Truncated internal cable network
- ODF/DDF (Optical Distribution Frame/Digital Distribution Frame) bandwidth
- Cross Connection to a number of Tier 1 carriers
- Internal inventory systems track all cables, circuits and cross-connects
- Scalable architecture including multiple redundant core switches and routers

5. **Technical Support & Services**

- On site technical engineers 24 x 7

- On site Network Operations Centre (NOC)

The processes and policy in place to prevent DoS attacks and application layer attacks.

1. The first (and possibly most important) stage in preventing a denial of service attack is to be aware when an attack is taking place. A key indicator would be a sudden spike in incoming traffic. All our servers are actively monitored and we will soon know if something is right. We will receive a notification from our server monitoring tool (such as Nagios) should any client exceed the maximum allowed requests in a given time period this will be visually flagged and a notification sent via email.
2. We also run an application called fail2ban on our Linux machines which performs a similar role but rather than being a monitoring tool this will actively disconnect and ban (usually for a period of 30 minutes in the first instance, increasing if the problem persists). It's important we set these limits correctly and these will be based on your expected usage, we can also add white lists (for example if a large number of users are based at one site using the same external address).
3. Over 70% of web attacks are carried out at the application level and so it's important that measures are in place to reduce this risk. Web application firewalls are used to establish an external layer that increases security and detects (as well as prevents attacks) before they reach the web application. For this we use ModSecurity, which is an open source intrusion detection and prevention system. We use the Open Web Application Security Project (OWASP) rules.
4. OWASP is a group of security communities that develops and maintains a free set of application protection rules, this is called the OWASP ModSecurity Core Rules Set (CRS). You can think of OWASP as an enhanced core rule set that the ModSecurity will follow to prevent attacks on the server.

Data transfer strategy if applicable (migrating existing systems).

1. Ideally, we would use the same mechanism as our backup strategy for this process which is rsync over ssh. This will provide a secure connection and allow us to re-sync the data should there be any disruption in the connection or if we plan to continue to use the existing platform whist testing is undertaken on the new platform. This option is of course dependant on the level of access we are granted to the current platform.
2. An alternative approach would be for the existing provider to supply us with encrypted zip files of your data which we would could transfer by secure ftp to the new server.

Bandwidth usage and scalability

1. The system which we are proposing will be extremely saleable and versatile, we are able to provide consistent performance for many concurrent users whilst maintaining an efficient pricing model. Our cluster utilises a pool of 3.2Ghz Quad Core E3-1230v2 systems to ensure optimal single core operation which is specifically suited to Apache, PHP and MySQL applications (depending on package you will have additional cores).
2. We have chosen the higher clock speed CPU's based upon our extensive experience with MySQL and Apache, MySQL in particular is not multi-threaded for single actions which means a higher clock speed and fewer cores is preferable once we reach 4 cores. For this reason we have gone with the

above processor. This will result in faster individual queries versus a slower clock speed CPU with more threads. There are a number of instances in Moodle/Totara and Mahara where this is advantageous (such as backup and restore of courses and statistics gathering).

3. In the unlikely event you exceed your bandwidth allocation it will automatically be extended and then reviewed, we can then determine if this is likely to happen in the future and if so move to the next price point which is an unlimited package. We will also be able to advise you on potential bandwidth saving options such as video compression techniques or look to provision a media server should the need arise.

External Access

1. External access will be granted based on the requirements of any internal contacts and external agencies; we will ensure that the access granted only provides access to parts of the system required by that agency or user. We can add their connection address to the allowed list (by IP, we can also enter a range if necessary) on the server and will request an SSH key for authentication. If terminal access is not required we will use a secure ftp account similar to the one used by yourselves with access to whichever areas are agreed by all parties.

Shared hosting

1. Our shared hosting environment sits on the same infrastructure as above with an additional layer to provide individual hosts on a single VM using nested virtualisation technologies. We use VMware, Webmin and Virtualmin to achieve this.
2. The Webmin module is used for managing multiple virtual hosts through a single interface, like Plesk or Cpanel. It supports the creation and management of Apache virtual hosts, BIND DNS domains, MySQL databases etc.
3. Virtualmin can also create a Webmin user for each virtual server, who is restricted to managing just his domain and its files. Webmin's existing module access control features are used, and are set up automatically to limit the user appropriately. Each individual domain will have their own server configuration files and individual instance of apache, php and MySQL allowing us to set site specific variables, install certificates and ensure data is not accessible to any other users on the platform.

Security and updates

1. All servers will be kept up to date with the latest security patches and updates, every effort will be made to prevent any unwanted access to our systems, such as, but not limited to:

    - Setting max password login attempts per session
    - Enabling auditd Services
    - Enabling a high quality, secure password policy
    - Limiting the reuse of passwords
    - Pruning Idle Users
    - Setting deny for failed password attempts
    - Use of firewalls (hardware and software)

- Use of antivirus where appropriate

Issue Date	Revision Number*	Revision Date*	Revision Changes*	Initials
01/10/09	-	-	Issued	KC
01/10/09	6	06/03/15	Not recorded	KC
01/10/09	3	08/05/2018	Changes to state our commitment to GDPR	EK, IH