Data Protection, Secure Hosting and Development Policy

Contents

GDPR Compliance

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:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. 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;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. 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;
e. 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
f. 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

a. This policy applies to all personal data processed by TDM.
b. The Responsible Person shall take responsibility for TDM's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. TDM shall register with the Information Commissioner's Office as an organisation that processes personal data.

Lawful purposes

a. Individuals have the right to access their personal data and any such requests made to TDM shall be dealt with in a timely manner.
b. 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).
c. TDM shall note the appropriate lawful basis in the Register of Systems.
d. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
e. 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

a. 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.
b. 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

a. TDM shall take reasonable steps to ensure personal data is accurate.
b. 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

a. To ensure that personal data is kept for no longer than necessary, TDM shall put in place an archiving

policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

Security

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

Breach

a. 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

All production services are hosted in UK data centres on iomart's VMware vCloud Director (VCD) platform. Administrative access is available via the VCD portal and Barracuda VPN (Windows and Linux clients). Platform resilience (compute, storage and networking) is provided by the hosting provider under our managed service.

VM-level backups are managed by iomart/RapidSwitch and the VCD toolset. TDM schedules quarterly full-VM restore tests and monthly local database restore tests. (Credentials and operational runbooks are held in NordPass and the internal handbook).

Storage

Under the managed VCD service, storage provisioning, availability and replication are delivered by the hosting provider. TDM does not maintain customer-visible LUN/iSCSI configurations in the current platform. Storage SLAs and resilience are covered by the hosting contract and provider documentation.

Vendor Certifications

Our hosting vendor holds ISO 27001 and 9001 accreditations.

Maximum Security

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

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

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

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

Technical Support and Services

- On site technical engineers 24 x 7
- On site Network Operations Centre (NOC)

Vulnerability Management and Protective Monitoring

We run an application called fail2ban on our Linux machines which will actively disconnect and ban any unknown connection attempts or multiple failed password attempts (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).

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. Our cluster is protected by a perimeter firewall which is configured to deny access to all by default, only necessary ports, services and destinations are then allowed.

All of our hosted servers are running in VMWare which has extensive tools for monitoring a plethora of information about our systems, this information is available in the forms of logs, statistics and graphs which can be seen in either real time or reflective / previous timeframes. We may also run additional reporting tools depending on the type of server being supplied. Many of our systems use AWStats reporting.

We use a variety of sources to gather information about potential threats, this can be either from our own systems (via logs, statistics and alerts), through client reports or through the media. We also actively review the red hat security channels for any pertinent information, all of our hosted servers run on CentOS.

Data Transfer Strategy

For migrations, TDM uses secure, resumable transfer methods (e.g., rsync over SSH or provider-mediated secure upload). Where third-party constraints apply, encrypted packages may be exchanged over secure channels. Exact method is selected per project and aligned with the hosting provider's capabilities on VCD.

Bandwidth Usage and Scalability

Capacity (compute, memory, bandwidth and storage) is provisioned elastically within the VCD environment. Performance and scaling are managed jointly by TDM and the hosting provider to meet demand without fixed hardware dependencies. No explicit bandwidth caps apply under the current contract.

External Access

Administrative access is only via Barracuda VPN (Windows and Linux clients).
· RDP: internal IPs only after VPN; no public RDP listeners.
· SSH: internal IPs after VPN; keys/credentials held in NordPass.
Any third-party access (e.g., BAES) is coordinated via Microsoft Teams sessions with agreed personnel and time-boxed scope.

Application Hosting (Virtualmin/Webmin)

Application sites are hosted on two Virtualmin/Webmin VMs (Hosting and Pensions) within VCD. Each Virtualmin instance manages separate virtual servers (vhosts), databases and TLS for its domains.
Administration is via Webmin/Virtualmin on internal IPs over VPN; site credentials and entry titles are

recorded in NordPass. No generic public shared hosting tier is used.

Security and Updates

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

Configuration and Change Management

The purpose of our change management system is to ensure that every change request is received, analysed and then either approved or rejected. If it is approved any other project constraints will be reviewed for possible impact. Impact factors include, but are not limited to;

- Financial constraints / budget
- Scheduling / resource availability
- Security
- Compatibility
- Feasibility

Our configuration management process will ensure that all parameters are identified and analysed for any impact on the existing system. Our experience over the past decade in working with the platforms we support ensure we are well placed to assess these factors whether it be Moodle, Totara, Mahara or other open source systems. A solid approach to change management is essential when working with any system but particularly so when code is General Public License (GPL).

Secure Software Development

All of our development activities and customisations are tracked using the git repository, we host our own gitlab environment which enables us to have complete control over project development, tracking and collaboration. “GitLab enables portfolio planning and management through epics, groups (programs) and milestones to organize and track progress. Regardless of your methodology from Waterfall to DevOps, GitLab’s simple and flexible approach to planning meets the needs of small teams to large enterprises. GitLab helps teams organize, plan, align and track project work to ensure teams are working on the right things at the right time and maintain end to end visibility and traceability of issues throughout the delivery lifecycle from idea to production.” – https://about.gitlab.com

Incident Management

ITIL defines an incident as an unplanned interruption to or quality reduction of an IT service. The service level agreements (SLA) define the agreed-upon service level between the provider and the customer.

An indent is handled differently to a problem or request, an incident interrupts normal service for large numbers / all users. We will often be aware of an incident before you are and, in this situation, we will endeavour to inform you as soon as possible the reason for the outage and expected timeframe to resolve the issue. This will either be communicated via our helpdesk, email or over the telephone depending on the number or users affected and the circumstances of the incident.

Our incident management approach is closely aligned to our service desk which will be your main point of contact with us. We operate a manned helpdesk during office hours and have an emergency contact number for out of hour critical incidents. We also have a 24/7 online portal which can be used to log non-critical faults, these will be reviewed as per our service agreement (4 hours non-critical during office hours), tickets will be prioritised into one of three categories (high, medium, low) and one of two departments (support /

change request). Critical incidents should be logged on the system, but it is imperative that you speak to a member of staff to ensure an immediate response. We have service level agreements with our hosting provider who have staff on site 24/7.

When a service fails, is interrupted or is unable to deliver the promised performance during normal service hours it is essential to restore the service to normal operation as soon as possible. Any condition that has the potential to result in a breach or degradation of service ought to trigger a response that prevents the actual disruption from occurring.

New incidents are often like incidents that have happened previously. Our incident model defines the following:

- Steps to be taken to handle the incident, sequence and responsibilities
- Precautions to be taken prior to resolving the incident
- Timescales for resolution
- Escalation procedures
- Evidence preservation

Cyber Certifications Held by TDM

IASME Governance
IASME Cyber Essentials

The Development Manager
Sector: Education
Certificate number:
Certificate level: Cyber Essentials
Date issued: 10/01/2025
Certification Body: IASME

The above certificate is currently held and renewed annually, next recertification 10/01/2026

Document Management

Document Name and Reference	Data Protection, Secure Hosting and Development Policy-TDMPP061
Classification	Internal & External
Policy Ownership	This policy is owned by all staff at TDM
Policy lead originator and point of contact in relation to its content:	Elizabeth Hoyos-Operations Director Ian Hatton - Academic & Technical Support Lead
TDM policy and procedure approval	Elizabeth Hoyos-Operations Director
Signature	
Date	01/02/22

Version Control					
Issue Date	Revision Number	Revision Date	Revision Changes	Initials	Next Revision Date

-	-	-	Issued	KC	
	6	06/03/15	Not recorded	KC	
	7	08/05/18	Changes to state our commitment to GDPR	EK, IH	
	8	28/08/19	Added changes to include enhanced security from vendors and for development of VLE platforms	IH, EK	
	9	17/02/21	Updates to server specifications, hosting policy and security devices. Added section “cyber certifications”.	IH	
	10	01/02/22	Updated Cyber Certifications	IH	
	11	28/09/23	Updated formatting Reviewed doc for changes	AR IH	Sept 2024
	11	01/02/24	Updated cyber certificate details	AR	Sept 2024
	11	09/09/24	Reviewed – no changes	IH	Sept 2025
	12	21/12/25	Rewrite for new hosting platforms	IH	Dec 2026