EUROPEAN ACADEMY OF ADVANCED STUDIES

113 Mindo, Triq L-Imdina, Qormi, QRM 9016, Malta

DATA PROTECTION POLICY

GDPR (EU) 2016/679 and the Data Protection Act (Cap. 586, Laws of Malta)

Document Control

Field	Detail
Document title	EAAS Data Protection Policy
Reference	Appendix 9.3
Owner	Data Protection Officer, EAAS
Approved by	[Board / Academic Council]
Version	2.0
Effective date	20.09.2024
Next review	01.01.2027
Applies to	All staff, students and parties process data for EAAS

Contents

1. Purpose

Every day the European Academy of Advanced Studies ("EAAS" or "the Academy") handles information about the people it works with – students applying and studying, staff it employs, and partners it deals with. This policy explains how we look after that information and sets the standard everyone here is expected to meet.

EAAS delivers its programmes entirely online. Because our teaching, assessment, student records and administration all depend on digital systems, protecting personal data is inseparable from keeping those systems available and recoverable. For that reason, this policy does two things at once: it sets out how we comply with data protection law, and it sets out the backup arrangements and automated continuity procedures that keep our service running – or bring it back quickly – when equipment or software fails.

We are bound by the General Data Protection Regulation (EU) 2016/679 (the "GDPR") and by the Data Protection Act, Chapter 586 of the Laws of Malta, together with the regulations made under it. Beyond simply meeting those rules, the Academy wants the people whose data we hold to feel confident that it is treated carefully, used only for good reasons, kept safe, and available when it is needed.

2. Scope

This policy covers all personal data the Academy processes, whatever form it takes – on a server, in a cloud service, in an email, or on paper – and wherever it is stored or accessed.

It binds everyone who handles personal data on behalf of EAAS: students and applicants, alumni, faculty, employees, contractors, volunteers and any third party acting for us. It reaches across the systems we rely on – the learning management system (LMS/VLE), the student information system, email and collaboration tools, the website, CCTV, and the cloud infrastructure behind them – and it governs the backup, redundancy and disaster-recovery measures that protect those systems. Reading and following this policy is part of studying, working or otherwise engaging with the Academy.

3. Key Terms

A few terms are used throughout, and it helps to be clear about them from the outset.

Term	What it means
Personal data	Any information relating to a living person who can be identified from it.
Special category data	More sensitive information – health, racial or ethnic origin, religious beliefs, biometric data and the like (GDPR Art. 9) – which needs extra care.
Processing	Practically anything done with data: collecting, storing, using, sharing or deleting it.
Controller	Whoever decides why and how data is processed. For the data covered here, that is EAAS.
Processor	An outside supplier that handles data on our instructions, such as a cloud or LMS provider.

Term	What it means
Data subject	The person the data is about.
Consent	A clear, freely given 'yes's to a specific use of data.
Personal data breach	Any incident where data is lost, exposed, altered or accessed when it should not have been – including loss of availability.
Backup	A separate, recoverable copy of data kept so the original can be restored if it is lost or corrupted.
RPO	Recovery Point Objective – the maximum amount of data (measured as time) we are prepared to lose in an incident.
RTO	Recovery Time Objective – the maximum time a service may be unavailable before it must be restored.
DPO	The Data Protection Officer, who oversees compliance and answers data questions.
IDPC	The Information and Data Protection Commissioner, Malta's data protection regulator.

4. The Rules We Follow

Our obligations come from several places, and we read them together rather than in isolation:

- the GDPR, Regulation (EU) 2016/679, which sets the European baseline;
- the Data Protection Act (Cap. 586) and its subsidiary legislation, which apply the GDPR in Malta;
- the legislation governing higher education and the recognition of qualifications in Malta, and the requirements of the MFHEA, where they touch the data, we hold; and
- the guidance and decisions published by the IDPC and the European Data Protection Board, which we treat as authoritative.

5. The Principles Behind Everything We Do

Article 5 of the GDPR sets out seven principles. They are not a checklist to tick once; they shape every decision about data at the Academy.

Lawful, fair and transparent. We process data only where we have a proper reason to, and we are open with people about what we do.

Used only for the purpose collected. Information gathered for one reason is not quietly repurposed for another.

No more than we need. We ask for the minimum that does the job, and resist collecting data 'just in case'.

Accurate. We keep records current and put mistakes right promptly.

Kept no longer than necessary. Once data has served its purpose it is deleted or anonymized – the retention schedule in Section 12 spells out the periods.

Secure. Data is protected against loss, against corruption, and against people who have no business seeing it – which is why backup and continuity, in Sections 17 and 18, sit inside this policy.

Accountable. We can show, not just assert, that we meet these standards.

6. Why We Are Allowed to Process Data

We do not process personal data unless one of the lawful bases in Article 6 applies. In practice, our processing usually rests on one of the following:

- a contract – enrolling students, running programmes and managing staff all depend on it;
- legal obligations, such as accreditation, tax and statutory reporting;
- our legitimate interests in running, securing and protecting the Academy, weighed against the individual's interests;
- consent, for optional things like marketing or the use of someone's photograph; and
- vital or public interest, in rare cases (a medical emergency, say) where that is what applies.

The basis relied on for each activity is written down in our Record of Processing Activities (Section 16), so it is never left to guesswork.

7. Sensitive Data and Data About Children

Some information needs more than the ordinary level of protection. When we process special category data – typically health or disability information used to arrange accessibility support – we identify a further condition under Article 9, usually explicit consent or a substantial public interest, and we limit access tightly.

Where we handle data about minors, we take extra care: parental or guardian consent is obtained where Maltese law requires it, and anything we ask a young person to read is written plainly.

8. Whose Data We Hold, and What

We collect data for academic, administrative, contractual and legal reasons only, and no more of it than those reasons call for. The main groups, and the kinds of information involved, are:

People	Typical information held
Students and applicants	Name, contact details, date of birth, ID or passport, nationality, prior qualifications, academic records and results, fees and payment data, and any accessibility needs.
Faculty and staff	Name, contact details, ID, employment and qualification records, payroll and bank details, and performance information.
Alumni	Name, contact details, and the record of what they studied and when they graduated.

People	Typical information held
Visitors and website users	Name and contact details, CCTV images, IP, cookie and usage data online.

9. Consent

When we rely on consent, it must be a genuine, active choice. A pre-ticked box or a failure to object does not count. We tell people clearly what they agree to, keep a record of what they were told and when, and make withdrawing consent as straightforward as giving it was. Withdrawing consent stops future processing; it does not unwind what was lawfully done beforehand.

10. Your Rights Over Your Data

The GDPR gives individuals real control over their information, and the Academy honours each of these rights:

- to be informed about how their data is used, through our privacy notices;
- to see a copy of the data we hold about them;
- to have it corrected when it is wrong or incomplete;
- to have it erased, where no legal duty requires us to keep it;
- to restrict or object to certain processing, including direct marketing; and
- to portability, and not to be subject to solely automated decisions of legal effect.

Requests go to the DPO (Section 20). We reply within one month and only extend that – by up to two months, having told the person why – when a request is genuinely complex. There is normally no charge, and we always confirm who we are dealing with before releasing anything. The step-by-step procedure is in Appendix B.

11. Keeping Data Safe

Security is matched to the risk. The measures we rely on include:

- encryption in transit (TLS) and at rest (AES-256), with data held in approved EAAS systems rather than personal accounts or devices;
- access granted on a need-to-know basis, protected by strong, multi-factor authentication;
- routine patching and anti-malware, and network protections such as firewalls;
- pseudonymization or anonymization wherever it is practical;
- secure destruction of records, paper and digital alike, once they are no longer needed; and
- regular testing and review, because a control that worked last year may not be enough this year.

Backups and continuity are a core part of security – they protect the availability of data – and are dealt with in detail in Sections 17 and 18.

12. How Long We Keep Things

Data is not kept indefinitely. We hold it for as long as the purpose or the law requires, and no longer; when that time is up it is securely deleted or anonymized. The schedule below sets the working periods, subject to any longer term the law imposes.

Record	Kept for	Counted from
Student academic records and results	Indefinitely, so awards can be verified	Graduation or withdrawal
Applications that did not proceed	12 months	The decision
Enrolment and contract records	Study period plus 6 years	End of the relationship
Financial and payment records	As Maltese tax law requires (around 10 years)	The transaction
Employee records	Employment plus the statutory period	End of employment
Marketing consents	Until withdrawn	—
CCTV footage	30 days	Recording
Website and cookie logs	12 months	Collection
Backup copies	Rolling retention per Appendix C, then overwritten	Backup date

13. Sharing Data, and Sending It Abroad

Sometimes data must leave the Academy – results sent to a partner university, returns made to a government authority, payments handled by a provider. When that happens, we share only what the task requires, only where there is a sound administrative or legal reason, and always under the GDPR and any contract that applies. We keep a note of what was shared and why.

Data is not sent outside the European Economic Area unless the destination offers adequate protection in the Commission's eyes, or unless we have safeguards such as Standard Contractual Clauses in place. Because some of our cloud and backup infrastructure may involve providers with a global footprint, we confirm the location of stored and backed-up data and ensure a valid transfer mechanism covers it. Where transfers happen, the people affected are told.

14. Working With Suppliers

Where an outside supplier processes data for us – including the providers that host our LMS, student system, email and backups – we choose one that can show it takes data protection seriously, and we put a written agreement in place before any data changes hands. That agreement, required by Article 28, covers security, confidentiality, the use of

any sub-processors, breach of notification, and what happens to the data when the contract ends.

For providers that our service depends on to stay available, we also confirm their own resilience commitments – backup, redundancy, disaster recovery and uptime – in the contract or service-level agreement, and we give weight to independent assurance such as ISO/IEC 27001 or SOC 2 certification. Suppliers act on our documented instructions and nothing more.

15. Building Protection in from the Start

Data protection is easier and cheaper to get right at the design stage than to bolt on afterwards, so it is considered whenever we plan a new system, programme or process – and that includes how the system will be backed up and recovered. Where something we propose could pose a high risk to people – large-scale monitoring, or an untried technology, for instance – we carry out a Data Protection Impact Assessment first and consult the IDPC if the assessment shows we should.

16. Our Record of Processing

As Article 30 requires, we maintain a record of our processing activities: what we do with data, whose data it is, who receives it, where it goes, how long we keep it, and how we protect it – including where and how it is backed up. We keep the record up to date and make it available to the IDPC if asked.

17. Backup Systems and Data Resilience

Because EAAS operates entirely online, the availability of our data matters as much as its confidentiality: a student cannot learn, and staff cannot administer, from records that have been lost. This section sets out how the Academy backs up its data so that, whatever happens to a server, a service or a file, a good copy can be recovered.

17.1 Our backup strategy

We follow a "3-2-1" approach to every business-critical dataset:

- at least **three copies** of the data (the live copy plus two backups);
- held on **two different types of storage**, so a single technology failure cannot take out every copy; and
- with **at least one copy kept off-site** in a geographically separate location, so a local disaster does not destroy the backups too.

Backups are encrypted both in transit and at rest, stored only in approved EAAS or contracted-provider systems, and protected by strong, least-privilege, multi-factor-protected access. Where the platform allows, at least one recent copy is held as an immutable, write-once ("air-gapped" or object-lock) backup that cannot be altered or deleted for its retention period, so that ransomware or a rogue action cannot corrupt every copy at once.

17.2 What we back up, and how often

The backup frequency for each system is set by its Recovery Point Objective (RPO) – the most data we are willing to lose. The busier and more critical the system, the shorter the interval between backups. Appendix C holds the full schedule; the essentials are:

System / data	Backup method & frequency	Retention of backups
Learning management system (LMS/VLE) – courses, content, grades, forums	Continuous database transaction logging + automated daily full backup	35 days rolling, plus monthly archive
Student information system / student records	Automated daily incremental + weekly full; continuous transaction logs	90 days rolling, plus end-of-term archive
Email & collaboration (e.g. Microsoft 365 / Google Workspace)	Provider-native continuous protection + independent third-party backup, daily	30–90 days
Website & content-management system	Automated daily backup of files and database	30 days rolling
Financial and payment records	Automated daily backup	Retained to meet Maltese tax law
Configuration & infrastructure-as-code	Version-controlled; backed up on every change and daily	12 months of versions

17.3 Automated procedures

Backups do not depend on someone remembering to run them. They are automated, scheduled and monitored so that the routine happens on its own and the exceptions raise an alarm:

- scheduled jobs run automatically at defined times, with no manual step required for a normal backup cycle;
- after each run, the system automatically verifies the backup – checksums and integrity checks confirm the copy is complete and readable;
- automated monitoring watches every job, and any failure, missed run or capacity warning triggers an immediate alert to IT and, where relevant, the DPO;
- backup copies are versioned and retained on a rolling schedule, then securely overwritten when their retention period ends; and
- access to the backup systems is logged, restricted to named administrators, and separated from ordinary production access.

17.4 Restore testing

A backup is only worth having if it can be restored, so we test restores rather than assuming they work. On a defined schedule – at least quarterly for critical systems – the Academy performs a trial restore into an isolated environment, confirms the data is complete and usable, measures how long the restore takes against our recovery targets,

and records the result. Any restore that fails or runs slow is investigated and the backup process corrected.

18. Service Continuity and Disaster Recovery

Because our teaching is delivered online, an outage is not an inconvenience in the background – it interrupts learning directly. This section sets out the automated arrangements that keep the Academy running when equipment or software fails, and the plans that bring us back quickly when something more serious happens.

18.1 Recovery targets

For each service we set two targets: how quickly it must be back (the Recovery Time Objective, RTO) and how much data we can afford to lose (the Recovery Point Objective, RPO). Systems are grouped into tiers, and the targets are tighter for the systems students and staff cannot do without.

Tier	Examples	RTO (max downtime)	RPO (max data loss)
Tier 1 – Critical	LMS/VLE, student records, sign-in / authentication	≤ 4 hours	≤ 15 minutes
Tier 2 – Important	Email, website, finance & payments	≤ 24 hours	≤ 24 hours
Tier 3 – Supporting	Internal reporting, secondary tools	≤ 72 hours	≤ 24 hours

18.2 Automated resilience against equipment and software failure

The Academy's critical services are designed so that the failure of a single machine, disk or component does not take the service down. Wherever practical this is handled automatically, without waiting for a person to react:

- **Redundant, multi-zone hosting.** Critical systems run on cloud infrastructure spread across more than one availability zone, so the loss of one data center does not stop the service.
- **Load balancing.** Traffic is shared across multiple servers; if one instance fails, requests are routed automatically to the healthy ones.
- **Database replication and automatic failover.** Databases run with a live standby copy; if the primary fails, the standby is promoted automatically so service continues with minimal loss.
- **Automated health checks.** Monitoring continuous probes each service; when a check fails, the system automatically restarts, replaces or scales the affected component and escalates an alert to on-call staff.
- **No single point of storage.** Staff and students work in cloud-hosted, managed accounts rather than local-only files, so a failed laptop or phone loses no institutional data – the person simply signs in elsewhere.
- **Reversible software changes.** Updates are deployed through controlled processes that can be rolled back to the last known-good version if a release misbehaves.

18.3 Keeping teaching and learning going

If a primary platform becomes unavailable, the Academy does not simply wait. A defined fallback keeps students supported: essential materials are recoverable from backup and can be made available through an alternative channel, students are kept informed, and where an outage affects an assessment or deadline the Academy adjusts timings so that no student is disadvantaged by a failure that was not theirs.

18.4 Telling people during an incident

During a significant outage the Academy communicates promptly and plainly. A designated contact issues updates through channels that do not themselves depend on the failed system – for example a status notice, email or SMS – explaining what is affected, what is being done, and what students and staff should do in the meantime. If the incident is also a personal-data breach, the process in Section 19 runs alongside the recovery.

18.5 Invoking the plan, and who does what

The Academy maintains documented disaster-recovery runbooks – step-by-step instructions for restoring each critical system. A senior responsible person (typically the Head of IT, in consultation with the DPO and management) is authorized to declare an incident, invoke the plan, and coordinate recovery. Roles, contact details and escalation paths are recorded so that, when something fails, people know immediately who leads and what to do. Appendix D is a quick-reference summary.

18.6 Testing and review

Continuity arrangements are exercised, not just written down. The Academy runs a disaster-recovery test at least once a year – including failover drills and a tabletop walk-through of a realistic scenario – checks that recovery meets the RTO and RPO targets, and feeds every lesson learned back into the runbooks, the backup schedule and this policy. The resilience commitments of our hosting, LMS and backup providers are reviewed at the same time.

19. When Something Goes Wrong

No system is perfect, so it matters that breaches – including any loss of access or availability – are caught and handled quickly. Anyone who suspects a breach must tell the DPO straight away, using the form in Appendix A. It is always better to report and be wrong than to stay quiet.

The DPO then assesses what happened, contains it, and records it – every breach is logged, whether it must be reported further. If the breach is likely to put people's rights at risk, the DPO notifies the IDPC without undue delay and, where feasible, within 72 hours of the Academy becoming aware of it. If the risk to individuals is high, those individuals are told directly, in plain language, so they can protect themselves. Once the dust settles, we review what happened and fix whatever let it happen.

20. Who Is Responsible

Data protection and service continuity are a shared responsibility, but it is not vague – each role carries clear duties.

Role	What they are responsible for
EAAS (the controller)	Standing behind the policy and giving data protection, backup and continuity the resources they need.
Data Protection Officer	Advising the Academy, monitoring compliance, handling requests and breaches, and being the point of contact for the IDPC.
Head of IT / IT function	Running the backup, redundancy and disaster-recovery arrangements, monitoring them, and testing that they work.
Managers and heads	Making sure their teams process data properly and have been trained.
Everyone else	Using data only as authorized, keeping it safe, working in approved systems, and reporting anything that looks wrong.

21. Training and Awareness

Good intentions are not enough without knowledge to back them up. Everyone who handles personal data is trained when they join and again at regular intervals, and we run awareness activities – covering data protection, security and how to report a problem – to keep the subject, and any changes in the law, fresh in people's minds.

22. Getting in Touch, and Complaining

Any question, request or concern about personal data should go to the Academy's Data Protection Officer:

EAAS Data Protection Officer	Details
Name	-
Email	dpo@eaas.mt or info@eaas.mt
Phone	+356 21688898
Address	113 Mindo, Triq L-Imdina, Qormi, QRM 9016, Malta

If someone is unhappy with how we have handled their data, they can also take the matter to the regulator:

Information and Data Protection Commissioner	Details
Address	Floor 2, Airways House, High Street, Sliema SLM 1549, Malta
Phone	+356 2328 7100
Email	idpc.info@idpc.org.mt

Information and Data Protection Commissioner	Details
Online	idpc.org.mt – complaints can be filed through the website

23. Keeping This Policy Current

We look at this policy at least once a year, and sooner if the law, our systems or the way we work change enough to warrant it. Backup schedules and recovery targets are reviewed together with them. When it is updated, management signs off the new version and we let everyone affected know through the usual channels.

24. Compliance

Following this policy is not optional. Failing to do so can lead to disciplinary action – up to dismissal or exclusion from the Academy – and, under data protection law, can carry personal consequences too. EAAS takes that seriously and applies the same expectations at every level of the institution.

Appendix A – Breach Report Form

Complete this and send it to the DPO as soon as a breach is suspected – don't wait for certainty.

Field	Entry
Reported by / role	
When discovered	
When the breach occurred	
What happened	
Systems / data and people affected	
Roughly how many	
Availability affected? (outage / data loss)	
Likely impact	
What's been done so far	
Notify the IDPC?	Yes / No – if yes, when
Notify those affected?	Yes / No – if yes, when

Appendix B – Handling a Data Subject Request

1. Log up the request and note the date it arrives.
2. Confirm the requester's identity before anything is disclosed.

3. Acknowledge it and check the scope with them if it isn't clear.
4. Gather the relevant data from every system that might hold it – including backups where in scope.
5. Redact anything about third parties, or anything exempt.
6. Reply within a month – or up to three for a complex request, having told them so.
7. Record the outcome and keep the response on file.

Appendix C – Backup & Recovery Schedule

This schedule is maintained by the IT function and reviewed with this policy. Figures are indicative defaults to be confirmed against provider capabilities and operational need.

System	Backup type	Frequency (RPO)	Backup retention	Restore test
LMS / VLE	Full + transaction logs	Continuous / daily	35 days + monthly archive	Quarterly
Student records (SIS)	Incremental + weekly full	Daily / continuous logs	90 days + term archive	Quarterly
Email & collaboration	Provider + 3rd-party backup	Continuous / daily	30–90 days	Half-yearly
Website / CMS	Files + database	Daily	30 days	Half-yearly
Financial records	Full	Daily	Per tax law	Half-yearly
Configuration	Versioned repo + snapshot	On change / daily	12 months	Annually

Appendix D – Service Continuity Quick Reference

A one-page prompt for the first minutes of an incident. Full instructions are in the disaster-recovery runbooks.

Step	Action
1 Detect	Automated monitoring alert, or a report from staff/students, flags a failure.
2 Assess	Head of IT (with DPO) confirms scope, tier and whether personal data is affected.
3 Declare	If a Tier 1/2 service is down, declare an incident and invoke the DR runbook.
4 Contain & recover	Fail over to redundant systems or restore from the latest verified backup.
5 Communicate	Issue updates via a channel independent of the failed system; keep students informed.

Step	Action
6 Breach check	If personal data is compromised, run the Section 19 breach process (72-hour clock).
7 Restore & verify	Confirm the service is fully back and data is complete against RTO/RPO targets.
8 Review	Record the incident, hold a lesson-learned review, and update runbooks and this policy.

Incident roles	Contact
Incident lead (Head of IT)	
Data Protection Officer	dpo@eaas.mt
Management sponsor	
Primary hosting / cloud provider	
LMS provider	

Appendix E – Useful Contacts

Contact	Details
EAAS	113 Mindo, Triq L-Imdina, Qormi, QRM 9016, Malta · +356 21688898 · info@eaas.mt
Data Protection Officer	dpo@eaas.mt
Head of IT / incident lead	
IDPC (regulator)	