EUROPEAN ACADEMY OF ADVANCED STUDIES

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

IT POLICY

Acceptable use, security and management of the Academy's IT systems

Document Control

Field	Detail
Document title	EAAS IT Policy
Reference	Appendix 9.2
Owner	Head of IT, EAAS
Approved by	[Board / Academic Council]
Version	2.0
Effective date	20.09.2024
Next review	01.01.2027
Applies to	All students, staff and others using EAAS IT systems

Contents

1. Purpose

The European Academy of Advanced Studies ("EAAS" or "the Academy") runs on its IT systems. Teaching, learning, research and the day-to-day business of the institution all depend on them being available, reliable and safe to use. This policy sets out how those systems are meant to be used and looked after, and what we expect of everyone who touches them.

It is written to be read, not just filed. If you use an EAAS account, log into the learning platform, or pick up an Academy laptop, the rules here apply to you, and a few minutes spent understanding them saves a great deal of trouble later.

2. Scope

This policy applies to every IT system the Academy provides or controls – the learning management system, email, cloud storage, online learning tools, networks, servers and the devices we issue – and to everyone who uses them: students, faculty, staff, contractors and guests alike.

It also applies when those systems are reached from somewhere else: from home, from a personal phone, or over a public network. The location changes; the responsibilities do not.

3. Key Terms

Term	What it means
IT systems	All hardware, software, networks, accounts and services provided or managed by EAAS.
User	Anyone with access to EAAS IT systems, whatever their role.
Credentials	The username, password and any second factor that prove who you are to a system.
LMS	The learning management system (Moodle) used to deliver and manage courses.
Endpoint	Any device that connects to our systems – laptop, desktop, phone or tablet.
Security incident	Anything that threatens the confidentiality, integrity or availability of data or systems.
IT Helpdesk	The first point of contact for accounts, access and technical problems.

4. Who Does What

Keeping the Academy's IT safe is a joint effort, but the parts people play are different.

Role	Responsibility
EAAS management	Backs this policy, sets priorities and makes sure IT has what it needs to do the job.
IT department	Runs and protects the systems, manages accounts, applies updates, handles incidents and supports users.

Role	Responsibility
Heads of department	Make sure their teams know the rules and request the right access for the right people.
All users	Use systems sensibly, protect their credentials, and report anything that looks wrong.

5. Accounts and Passwords

Each person gets their own account, and that account is personal. Sharing a login – even with a colleague you trust, even 'just this once' – is not allowed, because once two people use one account, nobody can say for certain who did what.

A few rules keep accounts secure:

- choose a strong, unique password and never reuse it on other sites;
- keep it to yourself – IT will never ask you for it, and any message that does is a scam;
- turn on multi-factor authentication where it is offered, and treat it as the norm rather than an inconvenience;
- lock your screen when you step away; and
- tell the Helpdesk at once if you think someone else knows your password.

Accounts are created when someone joins, adjusted when their role changes, and disabled promptly when they leave. Trying to reach systems or data you have not been given access to is treated as a serious matter, whatever the motive.

6. Using EAAS Systems Responsibly

The Academy's systems are provided for academic, research and administrative work. That is what they are for, and what they should mostly be used for.

Everyone is expected to respect copyright, licensing and intellectual property – that means not copying software, papers or media you have no right to, and not passing off others' work as your own. Installing software, or changing how a system is set up, needs the IT department's approval first; this is not bureaucracy for its own sake but the only way to keep the estate secure and supportable.

7. Email, Internet and Communications

Email and messaging carry the Academy's name, so use them professionally. Be wary of unexpected attachments and links – phishing is the most common way attackers get in, and a moment's caution stops most of it. When in doubt about a message, don't click; ask the Helpdesk.

Reasonable, occasional personal use of email and the internet is fine, as long as it stays modest and doesn't get in the way of work or study. What is never acceptable is using Academy systems to view, store or send material that is illegal, harassing, discriminatory or otherwise inappropriate.

8. Software, Licensing and Equipment

We use licensed software and keep track of what is installed where. Only software approved and, where needed, licensed by the Academy belongs on EAAS devices. Pirated or unlicensed programs are both a legal risk and a common source of malware, so they have no place here.

Equipment issued to you remains the Academy's property and should be looked after accordingly – kept physically secure, not left unattended in public, and returned when you leave. Report loss or theft to the Helpdesk straight away so the device can be locked or wiped.

9. Remote Working and Personal Devices

Working remotely is normal, and so is using a personal phone or laptop to check email or join a class. When you do, the same care applies as on campus: keep your device updated, protect it with a passcode or biometric lock, and avoid handling sensitive data over open public Wi-Fi without a secure connection. Don't save Academy data to personal accounts or unmanaged drives – keep it in the approved EAAS systems where it can be protected and backed up.

10. Keeping Systems Secure

Behind the scenes, the IT department maintains the defences that keep the Academy running: firewalls and network controls, anti-malware on endpoints, prompt installation of security updates, and monitoring for unusual activity. Users have a part to play too – by not switching off security tools, not plugging in unknown USB devices, and not trying to work around controls that seem to be in the way. If a control genuinely blocks legitimate work, the answer is to raise it with IT, not to bypass it.

11. Data Security and Classification

All data held on EAAS systems is protected under the GDPR and the Data Protection Act (Cap. 586), and is handled in line with the Academy's Data Protection Policy. Sensitive information – personal data, financial records, anything confidential – must be encrypted and stored securely, and shared only with people who have a genuine need to see it.

If you come across data that seems to be exposed, or you suspect a breach or weakness of any kind, report it immediately (Section 15). Reporting early, even on a hunch, is always the right call.

12. Digital Learning Platforms

Teaching and learning are delivered through a set of approved platforms – Moodle, Zoom, BigBlueButton, H5P and others the Academy adopts. Access to courses and resources runs through these, alongside the digital library, and is governed by this policy and the library's own rules.

The Academy monitors how these platforms are used, both to protect them and to uphold academic integrity. That monitoring is proportionate and exists to keep the learning environment fair and secure, not to look over anyone's shoulder.

13. Using AI Tools

Generative AI tools are now part of how people work and study, and the Academy does not pretend otherwise. They may be used where doing so is permitted and properly acknowledged. Two cautions matter most: never paste personal, confidential or unpublished Academy data into a public AI service, since you lose control of it once you do; and remember that AI output can be wrong, so it is checked, not trusted blindly. Where a programme sets its own rules on AI in assessment, those rules take precedence.

14. Backup and Recovery

Critical data is backed up automatically and regularly, and the IT department maintains procedures to restore systems and data after a failure. Backups are tested, because a backup that has never been restored is only a hope. Users help by keeping their important work in the approved Academy systems rather than only on a local drive – files saved solely to a laptop are not covered by the central backups and can be lost for good if the device fails.

15. When Something Goes Wrong

Lost a laptop, clicked a link you shouldn't have, noticed an account behaving oddly? Tell the Helpdesk as soon as you can, using the form in Appendix B if it helps. Speed matters far more than blame: most incidents are contained easily if they are caught early, and the Academy would always rather hear about a problem than discover it later. Where an incident involves personal data, it is handled together with the Data Protection Officer under the Data Protection Policy, including any notification to the IDPC.

16. What's Not Allowed

Most of this policy is about doing things well. This section is the short list of things you must not do. Using EAAS systems, you must never:

- try to bypass, disable or defeat any security control;
- introduce malware, or knowingly do anything that puts systems or data at risk;
- access, copy or alter data you have no authorisation to touch;
- share your credentials or use someone else's;
- use the systems for anything illegal, or to harass, bully or discriminate against others; or
- let personal use grow to the point where it interferes with the Academy's work.

17. Monitoring

To keep its systems secure and this policy honoured, the Academy reserves the right to monitor and log the use of its IT – network traffic, system access, email where necessary, and platform activity. This is done lawfully and proportionately, in line with the Data Protection Policy, and the information gathered is used for security and compliance, not idle curiosity. By using EAAS systems, users accept that this monitoring takes place.

18. Breaking the Rules

Breaches of this policy are taken seriously and dealt with under the Academy's code of conduct and disciplinary procedures. Depending on what happened, that can range from a quiet word to formal disciplinary action, withdrawal of access, or, in serious cases, dismissal or exclusion – and where the law has been broken, referral to the authorities. Everyone is asked to acknowledge this policy when they enrol or are employed.

19. Keeping This Policy Current

Technology and the threats to it move quickly, so this policy is reviewed at least once a year, and sooner when a change in technology or the law calls for it. Updated versions are approved by management and shared with everyone through the usual channels.

Appendix A – Approved Platforms and Tools

The list below reflects the platforms currently approved for academic and administrative use. The IT department keeps it up to date; if a tool you need isn't here, ask before using it for Academy work.

Tool	Used for	Notes
Moodle (LMS)	Course delivery and management	Primary teaching platform
Zoom	Live online classes and meetings	Approved settings only
BigBlueButton	Virtual classroom	Integrated with the LMS
H5P	Interactive learning content	Within Moodle
EAAS email	Official communication	Academy accounts only
[Cloud storage]	File storage and sharing	Approved EAAS account

Appendix B – IT Incident Report Form

Send to the IT Helpdesk as soon as you notice a problem – don't wait to be sure.

Field	Entry
Reported by / role	
Date and time noticed	
System or device involved	
What happened	
Any data affected?	
Action taken so far	
Still ongoing?	Yes / No

Appendix C – Acceptable Use Acknowledgement

To be signed by every user on enrolment or employment.

I confirm that I have read and understood the EAAS IT Policy. I will use the Academy's IT systems responsibly and only as permitted, keep my account credentials secure, and report any security concern or incident promptly. I understand that misuse may lead to disciplinary action and, where relevant, legal consequences.

Name	Role / programme
Signature	Date

Appendix D – Useful Contacts

Contact	Details
EAAS	113 Mindo, Triq L-Imdina, Qormi, QRM 9016, Malta · +356 21688898 · info@eaas.mt
IT Helpdesk	[admin@eaas.mt] · virtual consultation on request
Head of IT	Hemand Thakur [admin@eaas.mt]
Data Protection Officer	Dr. Leul Girma Haylemariam · [dpo@eaas.mt] – for incidents involving personal data

This is an internal policy of the European Academy of Advanced Studies, written to guide everyday use of its IT systems. It should be read alongside the Academy's Data Protection Policy and code of conduct.