Information Technology Policy

Version	Date	Description	Reviewed / Approved By
1.0	Board Approved 7th Sept 2026	New I.T. policy	Omnisys, IT Manager, CEO.

This document provides an abridged summary of four key I.T. policies proposed by Athletics Ireland's current I.T. strategic partner, OmniSys and adapted by the Athletics Ireland I.T. Management Team. This policy also operates in partnership with our existing Business Continuity policy. It sets out the core governance requirements for I.T. compliance across Athletics Ireland, including acceptable use, asset management, remote and hybrid working, password and account security, and business continuity.

1. Policy Overview

This policy consolidates the key points from the following policy documents for ease of reference.

Policy Title	Key Areas Covered
Acceptable Use Policy	User responsibilities; prohibited use; expectations of privacy; personal use; reporting violations; remote work; bring your own device.
Asset Management Policy and Procedures	Responsibilities of individual employees; asset security; use of Athletics Ireland assets.
Remote Working Policy	Remote and hybrid working definitions; operating principles; employee responsibilities; I.T. arrangements; data security; insurance; health and safety; right to disconnect; e-working and tax relief.
Password Management Policy	Password and account security; account lockout; privileged accounts; password confidentiality; contractor accounts; account disablement.
Artificial Intelligence	It is essential to establish a cybersecurity policy for generative AI systems that defines the principles, standards, and best practices for ensuring the security and integrity of AI-generated content and data.

Note- All Athletics Ireland policies are reviewed every three years or sooner as required if legislation and best practice develops. We note the fast moving pace of information technologies and we embrace best practice.

2. Summary

This section summarises the key responsibilities for all users. All users refers primarily to Athletics Ireland staff but also all users of competition devices, systems, accounts, software and services. It is intended as a plain-English guide for all.

- Use only Athletics Ireland-approved devices, systems, accounts, software and services for Athletics Ireland work.
- Protect Athletics Ireland information, equipment and systems from loss, damage, unauthorised access or disclosure.
- Keep passwords confidential and do not use browser “remember password” features on Athletics Ireland systems.
- Store Athletics Ireland data only on approved Athletics Ireland platforms and devices.
- Do not connect personal devices, removable media or unauthorised equipment to Athletics Ireland networks without formal approval.
- Report lost or damaged equipment, suspected security incidents, data breaches or policy violations immediately to your line manager and the I.T. Manager.
- When working remotely, use a secure internet connection, protect confidential information, update your Outlook calendar and maintain normal working hours and duties.
- Respect colleagues’ right to disconnect outside normal working hours.

3. Acceptable Use Policy

3.1 User Responsibilities

1. Users must use only pre-approved Athletics Ireland assets, technology and services.
2. All Athletics Ireland assets are provided on loan to users so that essential job functions can be performed.
3. On leaving Athletics Ireland, or on contract termination, users must return all supplied I.T. assets, access Staff Cards and fobs, and associated data.
4. Users must secure the physical environment around their workstation and lock their computers when stepping away.
5. Users must ensure that personally identifiable information, confidential information and other sensitive data, including data covered by GDPR or other regulation, is not readily available or accessible at their desk or workspace, whether working in an Athletics Ireland office, at home or at another approved location.
6. Users must take appropriate care to protect information, systems and related assets in their custody from loss, damage or harm. Lost or damaged equipment must be reported to I.T. as soon as practicable.
7. Users must store passwords securely and keep them confidential.

8. User-assigned accounts must only be used to access assets, operating systems, applications, files and data for which access has been granted. The ability to inadvertently read, execute, modify, delete or copy data does not imply permission to do so. Users should report to their line manager and the I.T. Manager if they believe they have access to data they should not be able to access.
9. Only authorised users may post content or create the impression that they are representing Athletics Ireland on social networking sites, blogs or other internet sites.
10. Users must keep information and knowledge about Athletics Ireland information systems confidential during and after employment. Staff should refer to the Athletics Ireland Employee Handbook, July 2020, version 3 (currently under review).

3.2 Prohibited Use

1. Only approved and authorised devices may be connected to networks owned or managed by Athletics Ireland, including portable end-user devices, removable devices such as USB drives and personally owned devices.
1. Users must not share passwords or allow others to use their accounts. Users are responsible for all activity originating from their usernames and accounts.
2. Users must not circumvent user authentication mechanisms or the security of any user account or information system asset.
3. Users must not install software or hardware, or modify system configuration settings, on any Athletics Ireland asset without approval.
4. Users must not engage in any activity intended to disrupt Athletics Ireland assets or networks.
5. Users must not perform network monitoring, port scanning or security scanning unless this activity is part of their normal role and has been formally authorised.
6. Users must not use Athletics Ireland assets for personal economic gain.
7. Users should not use “Remember Me” or “Remember my Password” browser functions on Athletics Ireland systems.

3.3 Expectations of Privacy

1. When using Athletics Ireland resources, users should have no expectation of privacy, except where privacy is protected by law. Internet access, email, instant messaging and related communications may not be confidential.
2. Athletics Ireland reserves the right to monitor, access and disclose information generated and actions performed using Athletics Ireland I.T. assets. Files, messages, attachments and logs may be retained and used as evidence in litigation, audits and investigations.

3.4 Personal Use

1. Users are permitted limited personal use of Athletics Ireland assets, such as visiting websites and checking personal email accounts, provided this does not conflict with this policy or interfere with work duties.
2. Users must not access web-based personal password managers on Athletics Ireland assets. Local installation of a password manager must be approved by the I.T. Manager.
3. Users must not store Athletics Ireland passwords in personal password managers.
4. Users must not use browser sync or browser profiles in a way that transfers browser history between personal devices and Athletics Ireland assets.
5. Users must not use personally owned accounts, such as Apple ID, Google Account or Microsoft Account, as device-wide accounts on Athletics Ireland devices unless permitted by Athletics Ireland.
6. Employees must work with OmniSys and the I.T. Manager to create Athletics Ireland-specific accounts for required assets and third-party services.
7. Users must not use Athletics Ireland licence keys on personal devices unless authorised by the I.T. Manager.
8. Athletics Ireland data must not be stored on non-Athletics Ireland personal cloud platforms, such as Google Drive, personal Microsoft OneDrive or Dropbox.

3.5 Reporting Violations

Employees who become aware of any event that threatens the availability, integrity or confidentiality of Athletics Ireland data, breaches any standard, policy, procedure or related requirement, or may be contrary to law, must immediately contact their line manager and the I.T. Manager.

3.6 Remote Work and Approved Assets

1. All Athletics Ireland work must be performed on Athletics Ireland-approved assets.
2. All Athletics Ireland data must be stored on approved Athletics Ireland assets.
3. Employees must not connect Athletics Ireland assets to open or unencrypted Wi-Fi networks.
4. Employees must remain aware of their surroundings when working remotely to prevent shoulder surfing or unauthorised viewing of sensitive material.

3.7 Bring Your Own Device

This section sets out the restrictions and requirements that apply to the use of personal devices for work activities.

1. Personal devices must not be connected to the Athletics Ireland network without formal authorisation.
2. Athletics Ireland data must not be stored on personal devices without formal authorisation.
3. Where a personal device (i.e. a personal phone) is authorised to store Athletics Ireland data, Athletics Ireland data may be remotely wiped from the device if required.
4. Reasons for wiping Athletics Ireland data may include a lost or stolen device, termination of employment, or a compromised or hacked account or device.

4. Password and Account Security

1. New passwords must be implemented once initial OmniSys generated password is used to access all systems upon initial log in on an Athletics Ireland computer.
2. Password accounts must be reviewed quarterly, and inactive accounts must be disabled or deleted, as necessary.
3. Initial passwords for new users must be temporary and require the user to change the password at first login.
4. An account lockout policy is implemented for unsuccessful login attempts. Repeated incorrect login attempts must cause the account to lock. The current rolling scale is that five failed attempts will lock the user out for one minute, with further failed attempts extending the lockout period. Users must verify their identity as part of the process to release a locked account.
5. Users with privileged or super-user accounts must maintain these separately from routine user accounts, with separate user IDs and passwords. Privileged accounts must only be used when necessary and must not be used for standard access. Their use will be monitored.
6. All user passwords must be kept confidential and must not be recorded in any way that could allow others to access or identify them. Passwords must never be shared. Suspected password compromise must be reported as an Information Security Incident and the password must be changed immediately.
7. Employees, contractors and third-party users must receive appropriate training on effective password management, including how to select suitable passwords and safe usage practices such as not selecting “remember password” options.
8. Contractor accounts must be disabled on the expiration date of the contract.
9. Passwords that need to be communicated externally must be communicated by secure verbal communication or encrypted electronic communication only.
10. Screen-saver passwords must activate after five minutes of user inactivity. Users must not be permitted to change the inactivity period.
11. Administrative account passwords must be changed following the departure of staff who had access to those passwords, or where password compromise is suspected. User accounts must be disabled on departure of personnel.

12. Athletics Ireland must notify OmniSys as soon as an employee confirms they are leaving. A mutually agreed date will be confirmed with OmniSys for system access to be locked.
13. Passwords must not be embedded in automated programs, utilities or applications, such as batch files or terminal hotkeys.
14. Passwords must not be visible on screens, printed hard copies or any other output device.

5. Asset Management Policy

5.1 Responsibilities of Individual Employees

1. Employees must understand the value, importance and security requirements of Athletics Ireland assets, as communicated through the Athletics Ireland Information Security Training Policy, during induction and all subsequent I.T. system trainings.
2. Employees must use Athletics Ireland assets strictly in accordance with the Acceptable Use Policy and any other documentation issued in relation to specific assets.
3. Employees must report any potential or actual security weaknesses relating to Athletics Ireland assets and controls promptly through the correct communication channels, as detailed in the Athletics Ireland Information Security Incident Policy.

6. Defining Athletics Ireland I.T. Assets

Athletics Ireland uses a range of I.T. assets. Most are covered by this policy, although some specialist assets, such as servers and server rooms, may require additional controls managed by I.T. personnel.

For the purposes of this document, Athletics Ireland assets include end-user devices, network devices, non-computing or Internet of Things devices (access fobs), and servers in virtual, cloud-based or physical environments, (including assets that can connect remotely). Athletics Ireland assets are managed by OmniSys and the I.T. Manager. Each asset is identified by a unique asset identifier.

1. End-user devices, such as desktops, workstations, laptops, tablets and smartphones.
2. Network devices, such as wireless access points, switches, firewalls, physical or virtual gateways and routers.
3. Non-computing or Internet of Things devices – office access fobs and printers etc.
4. Servers, such as web servers, email servers, application servers and file servers.

7. Remote Working Policy

7.1 Definitions

Term	Definition
Remote work	An arrangement where an individual works at an alternative worksite to the employer's work premises.
Hybrid working	A working arrangement that combines working from the employer's premises and working remotely, based on agreement between the employee and manager and approval through the application process.

Athletics Ireland will continue to be the primary workplace for many staff. Employees may be required to attend the office on specific agreed days each week, for periods required to support Athletics Ireland business, for an agreed percentage of days each week or month, or on days required by their manager for collaboration, meetings, training and key events.

Any remote or hybrid working arrangement must be discussed and agreed between the employee and manager before approval. Employees will continue to work the same hours and perform the same duties as if they were in the office, unless otherwise agreed with their manager for specific events and times of the year.

General information on the Remote Working Policy is covered in the Athletics Ireland Staff Handbook.

7.2 Operating Principles

1. Not all roles are suitable for remote working. Suitability is subject to manager approval and may vary by department.
2. The employee's manager will approve the remote work location and agreed duration.
3. The I.T. Manager will ensure that all required Athletics Ireland assets are supplied and maintained as required for a remote work environment.

7.3 Employee Responsibilities

1. Employees must remain available to their manager during scheduled working hours and manage boundaries between work and personal life.
2. Professional conduct, confidentiality and compliance with Athletics Ireland policies must be maintained while working remotely.
3. Employees must obtain prior written approval from Athletics Ireland before working remotely from outside Ireland.
4. Employees should access work emails and files only on approved Athletics Ireland equipment provided by the I.T. Department.

5. When working from home, employees must be available to answer work-related calls on an Athletics Ireland-issued mobile phone where one has been provided.

7.4 I.T. Arrangements, Data Security and Company Equipment

1. Employees must be familiar with the Athletics Ireland Information Security Policy and Acceptable Use Policy.
2. Confidential information and personal data must be protected at the remote working location, including hard copy documents and handwritten notes. Athletics Ireland documents must be disposed of securely in the office and must not be placed in public or private waste facilities.
3. Athletics Ireland intellectual property must be protected when materials are taken to a remote working location.
4. Employees must not transfer company files to or from personal email accounts.
5. Company equipment, including laptops, phones, monitors and keyboards, must not be left unattended. Screens must not be visible to others outside the remote working location.
6. Company equipment must only be used by the person to whom it is assigned and must not be left unattended in a personal vehicle.
7. Company equipment must be used for Athletics Ireland business only and may be subject to further operational rules.
8. Lost or stolen Athletics Ireland equipment must be reported immediately to the I.T. Manager and line manager.
9. Failure to keep company equipment or confidential information secure will be treated as a serious matter and may result in disciplinary action.
10. All company equipment must be stored securely and returned immediately when requested by Athletics Ireland.
11. Employees must use a secure and reliable broadband connection and must be vigilant about the risks of public Wi-Fi.
12. Any I.T. questions or suspected data or confidentiality breaches must be reported immediately to the employee's line manager, the I.T. Manager and OmniSys.
13. If a work phone is issued, it should not be used for personal use where possible.
14. Employees must ensure that devices have necessary operating system, software and antivirus updates; are used in a safe location; are locked when unattended; and use effective access controls such as strong passwords and, where available, encryption.
15. Work email accounts must be used for work-related emails involving personal data. If personal email must be used in exceptional circumstances, contents and attachments should be encrypted and personal or confidential data should be avoided in subject lines.
16. Paper records must be kept secure, for example in a locked filing cabinet or drawer, and must not be left where they could be read by others, lost or stolen.

7.5 Right to Disconnect

Athletics Ireland respects employees' right to disconnect from work outside normal working hours. Employees are expected to take adequate breaks and to respect colleagues' right not to routinely engage with work communications outside normal working hours.

Such communication can be expressed on work email footers.

8. Artificial Technology Policy

Introduction

Generative AI systems are capable of creating realistic and diverse content, such as text, images, audio, and video, based on data and models. These systems have many potential applications and benefits, such as enhancing creativity, personalization, accessibility, and education. However, they also pose significant cybersecurity risks, such as generating fake or misleading content, compromising data privacy, and enabling malicious attacks. Therefore, it is essential to establish a cybersecurity policy for generative AI systems that defines the principles, standards, and best practices for ensuring the security and integrity of AI-generated content and data.

Authorized Use

This section outlines the authorized use of generative AI systems and their outputs within Athletics Ireland.

Generative AI tools and platforms may only be used for business purposes approved by Athletics Ireland. Such purposes may include content generation for marketing, program development, research, or other legitimate activities.

- Generative AI systems and their outputs should only be used for lawful and legitimate purposes, in accordance with the applicable laws, regulations, and policies.
- Users and stakeholders of generative AI systems should obtain the necessary permissions, licenses, and consents before using or sharing AI-generated content and data.
- Unauthorized or malicious use of generative AI systems and their outputs, such as generating fake or misleading content, compromising data privacy, or enabling malicious attacks, is strictly prohibited and may result in legal or disciplinary action.
- Users and stakeholders of generative AI systems are responsible for ensuring that their use of AI-generated content and data is authorized and compliant with this policy and other relevant policies and guidelines.

Policy Objectives

The main objectives of this policy are to:

- Protect the confidentiality, integrity, and availability of AI-generated content and data
- Prevent and detect the unauthorized or malicious use of generative AI systems
- Promote the ethical and responsible use of generative AI systems
- Enhance the awareness and education of the users and stakeholders of generative AI systems

Policy Scope

This policy applies to:

- All generative AI systems and their components, such as data, models, algorithms, and software
- All users and stakeholders of generative AI systems, such as developers, operators, consumers, and regulators
- All types and domains of AI-generated content and data, such as text, images, audio, and video

Policy Principles

The following principles guide the implementation and enforcement of this policy:

- Accountability: All users and stakeholders of generative AI systems are accountable for their actions and decisions regarding the use and management of AI-generated content and data
- Transparency: All generative AI systems and their outputs should be clearly labelled and disclosed as such, and the sources and methods of their creation should be traceable and verifiable
- Security: All generative AI systems and their outputs should be protected from unauthorized or malicious access, modification, deletion, or distribution, and any breaches or incidents should be promptly reported and resolved
- Quality: All generative AI systems and their outputs should be accurate, reliable, and consistent, and any errors or anomalies should be detected and corrected
- Privacy: All generative AI systems and their outputs should respect the privacy and consent of the data subjects and owners, and any personal or sensitive data should be anonymized or encrypted
- Integrity: All generative AI systems and their outputs should be authentic and trustworthy, and any fake or misleading content should be identified and flagged
- Ethics: All generative AI systems and their outputs should adhere to the ethical and legal standards and norms of the relevant domains and contexts, and any harmful or offensive content should be avoided or removed

Policy Standards

The following standards specify the minimum requirements and best practices for Athletics Ireland compliance with this policy:

- Data Security: All data used or generated by generative AI systems should be stored, processed, and transmitted securely, using encryption, authentication, authorization, and backup mechanisms
- Model Security: All models used or generated by generative AI systems should be developed, trained, tested, and deployed securely, using validation, verification, auditing, and monitoring mechanisms
- Output Security: All outputs produced or consumed by generative AI systems should be labelled, disclosed, and verified as such, using metadata, watermarking, hashing, and digital signatures
- Data Quality: All data used or generated by generative AI systems should be accurate, complete, and relevant, and any errors, biases, or inconsistencies should be corrected or mitigated
- Model Quality: All models used or generated by generative AI systems should be robust, reliable, and generalizable, and any errors, anomalies, or vulnerabilities should be detected or prevented
- Output Quality: All outputs produced or consumed by generative AI systems should be realistic, diverse, and consistent, and any errors, artifacts, or discrepancies should be minimized or eliminated
- Data Privacy: All data used or generated by generative AI systems should respect the privacy and consent of the data subjects and owners, and any personal or sensitive data should be anonymized or encrypted
- Model Privacy: All models used or generated by generative AI systems should respect the privacy and consent of the model developers and owners, and any proprietary or confidential information should be protected or obfuscated
- Output Privacy: All outputs produced or consumed by generative AI systems should respect the privacy and consent of the output creators and consumers, and any personal or sensitive information should be removed or redacted
- Data Integrity: All data used or generated by generative AI systems should be authentic and trustworthy, and any fake or misleading data should be identified and flagged
- Model Integrity: All models used or generated by generative AI systems should be authentic and trustworthy, and any fake or misleading models should be identified and flagged
- Output Integrity: All outputs produced or consumed by generative AI systems should be authentic and trustworthy, and any fake or misleading outputs should be identified and flagged
- Data Ethics: All data used or generated by generative AI systems should adhere to the ethical and legal standards and norms of the relevant domains and contexts, and any harmful or offensive data should be avoided or removed

- Model Ethics: All models used or generated by generative AI systems should adhere to the ethical and legal standards and norms of the relevant domains and contexts, and any harmful or offensive models should be avoided or removed
- Output Ethics: All outputs produced or consumed by generative AI systems should adhere to the ethical and legal standards and norms of the relevant domains and contexts, and any harmful or offensive outputs should be avoided or removed

Policy Enforcement

The following measures are taken to ensure the compliance and effectiveness of this policy:

- Education: All users and stakeholders of generative AI systems should be educated and trained on the security and ethical implications and challenges of generative AI systems and their outputs
- Assessment: All generative AI systems and their outputs should be regularly assessed and evaluated for their security and ethical performance and impact
- Review: This policy should be periodically reviewed and updated to reflect the latest developments and best practices in generative AI systems and their outputs
- Sanction: Any violations or breaches of this policy should be reported and investigated, and appropriate sanctions or remedies should be applied

Appendix A: Glossary

Term	Definition
Asset	Anything that has value to an organisation, including people, computing devices, I.T. systems, networks, software, virtual platforms and related hardware.
Asset inventory	A register, repository or comprehensive list of Athletics Ireland assets and specific information about those assets.
Asset owner	The department, business unit or individual responsible for an Athletics Ireland asset.
Cloud environment	A virtualised environment that provides on-demand network access to shared resources such as computing, storage, applications and services.
Athletics Ireland assets	Assets with the potential to store or process data, including end-user devices, network devices, non-computing or IoT devices and servers in virtual, cloud-based or physical environments.
End-user devices	I.T. assets used by members of the organisation, including laptops, smartphones, tablets, desktops and workstations.
Athletics Ireland asset identifier	A unique number or alphanumeric tag, often on a sticker, used to track an asset in an asset inventory.
Mobile end-user devices	Athletics Ireland-issued devices with wireless capability, such as smartphones and tablets.
Network devices	Devices required for communication and interaction between devices on a computer network, including wireless access points, firewalls, gateways, routers and switches.
Non-computing or IoT devices	Devices embedded with sensors, software or other technologies that connect and exchange data with other devices or systems.
Physical environment	Physical hardware components that make up a network, including cables and routers.
Portable end-user devices	Transportable end-user devices that can wirelessly connect to a network, including laptops, smartphones and tablets.
Remote devices	Athletics Ireland assets capable of connecting to a network remotely, usually from the public internet.
Servers	Devices or systems that provide resources, data, services or programs to other devices on a local or wide area network.
User	Employees, third-party vendors, contractors, service providers, consultants or any individual who operates an Athletics Ireland asset.
Virtual environment	An environment that simulates hardware so software can run without requiring the same amount of physical hardware.