# Security Statement

PUB-LEG-007 | Effective 27 July 2026 | 5 min read

Plain English overview
A public overview of the measures used to protect Mosey, its users and information.

## Chapter 1: Our Commitment to Security

Effective 27 July 2026

Plain English summary
Protecting your account and personal information is one of our highest priorities. While no online service can ever guarantee absolute security, Moseyaround Limited is committed to implementing appropriate technical and organisational measures to safeguard the confidentiality, integrity and availability of our systems and the information entrusted to us.

### 1. Purpose

This Security Statement explains the principles and practices that guide how Moseyaround Limited protects:

- member accounts
- personal information
- rewards systems
- cloud infrastructure
- websites
- mobile applications
- supporting services

It should be read alongside our:

- Privacy Policy
- Fair Play & Anti-Cheat Policy
- Terms & Conditions

### 2. Our Security Principles

Our security programme is built around the following principles:

- confidentiality
- integrity
- availability
- accountability
- least privilege
- defence in depth
- continuous improvement

These principles influence how we design, build and operate Mosey.

### 3. Security by Design

Security is considered throughout the development lifecycle of Mosey.

Where reasonably practicable, new features are designed with security in mind from the earliest stages rather than being added after development.

This may include:

- secure coding practices
- design reviews
- access control reviews
- security testing before release
- ongoing monitoring after deployment

## 4. Protecting Your Account

We take reasonable steps to protect member accounts against unauthorised access.

These measures may include:

- secure authentication
- encrypted communications
- account verification
- monitoring for suspicious login activity
- protection against automated attacks
- session management

Members also play an important role by keeping their passwords and devices secure.

## 5. Encryption

Where appropriate, information is protected using industry-recognised encryption technologies.

This may include:

- encryption during transmission between your device and our services
- encryption of sensitive information at rest where appropriate
- secure cryptographic protocols

Encryption helps reduce the risk of unauthorised access to information.

## 6. Cloud Infrastructure

Mosey uses professionally managed cloud infrastructure designed to provide:

- resilience
- scalability
- availability
- security

Infrastructure providers are selected following appropriate assessment and are expected to maintain suitable security standards.

## 7. Access Controls

Access to systems and personal information is restricted to authorised individuals who require access for legitimate business purposes.

Access may be controlled through:

- role-based permissions
- authentication requirements
- least-privilege principles
- regular permission reviews
- audit logging

## 8. Monitoring and Threat Detection

We monitor our systems to help identify:

- suspicious activity
- attempted unauthorised access

- service interruptions
- technical anomalies
- potential security incidents

Monitoring is intended to protect members and maintain the integrity of the Mosey platform.

### 9. Secure Development

When developing and maintaining Mosey, we aim to:

- keep software reasonably up to date
- address known security vulnerabilities
- review dependencies
- minimise unnecessary exposure of systems
- improve resilience over time

Security improvements are an ongoing process rather than a one-off activity.

### 10. Member Responsibilities

Members also help keep Mosey secure by:

- choosing strong passwords where applicable
- protecting authentication credentials
- keeping devices updated
- reporting suspected security issues promptly
- avoiding sharing verification codes or login details

## Chapter 2: Incident Response, Business Continuity & Final Provisions

Effective 27 July 2026

Plain English summary
Despite strong security measures, no online service can completely eliminate risk. If a security incident occurs, our priority is to contain the issue, protect members, restore services and learn from the event.

### 11. Security Incident Response

Moseyaround Limited maintains procedures for identifying, assessing and responding to security incidents.

Our response may include:

- investigating the incident
- containing any immediate risk
- protecting affected systems
- restoring services
- preserving evidence where appropriate
- reviewing the cause of the incident

Every incident is assessed according to its nature and potential impact.

### 12. Personal Data Breaches

Where a security incident involves personal information, we will assess whether it constitutes a personal data breach under applicable data protection law.

Where legally required, we will:

- notify the Information Commissioner's Office (ICO)

- notify affected individuals without undue delay where there is a high risk to their rights and freedoms
- take appropriate steps to reduce any potential impact
- review our procedures to reduce the likelihood of recurrence

## 13. Vulnerability Management

Technology evolves continuously, and so do security threats.

We aim to:

- monitor for newly identified vulnerabilities
- assess the risks they present
- apply updates or mitigations where appropriate
- review the effectiveness of implemented fixes

Not every update can be applied immediately, but we prioritise security according to the level of risk.

## 14. Business Continuity

We recognise that uninterrupted service is important to our members.

We therefore aim to maintain reasonable arrangements to support the continued operation of Mosey during unexpected events.

These arrangements may include:

- resilient cloud infrastructure
- service monitoring
- backup procedures
- documented recovery processes
- contingency planning

While we strive for high availability, uninterrupted access cannot be guaranteed.

## 15. Backups and Recovery

Where appropriate, important systems and information are backed up to support recovery following events such as:

- hardware failure
- software faults
- accidental deletion
- infrastructure outages
- cybersecurity incidents

Backups are managed in accordance with our operational and security requirements.

## 16. Third-Party Security

Many services used by Mosey are provided by trusted third-party organisations.

Before using a provider, we aim to consider factors such as:

- security capabilities
- reliability
- compliance with applicable laws
- contractual safeguards
- operational resilience

Although we expect our providers to maintain appropriate security standards, each organisation remains responsible for securing its own services.

## 17. Responsible Disclosure

We encourage responsible disclosure of genuine security vulnerabilities.

If you believe you have identified a security issue affecting Mosey, please contact:

security@moseyaround.com

When reporting a vulnerability, we ask that you:

- act in good faith
- avoid accessing information that does not belong to you
- avoid disrupting services
- provide sufficient information to help us investigate

Responsible reports help us improve the security of Mosey.

## 18. Security Awareness

Security is an ongoing process.

Moseyaround Limited is committed to regularly reviewing and improving its security practices in response to:

- emerging threats
- technological developments
- regulatory guidance
- lessons learned from incidents
- feedback from members and security researchers

## 19. Member Security Tips

Members can improve their own security by:

- using a strong, unique password where applicable
- enabling additional authentication features if offered
- keeping their devices and operating systems up to date
- installing software updates promptly
- being cautious of phishing emails or fraudulent messages
- never sharing verification codes or account credentials
- contacting us if they suspect unauthorised access

Security is most effective when both Moseyaround Limited and members work together.

## 20. Changes to This Security Statement

We may update this Security Statement from time to time to reflect:

- improvements to our security programme
- technological developments
- changes in law or regulatory guidance
- operational experience

Where significant changes are made, we will update the Effective Date and provide notice where appropriate.

## 21. Contact Us

For security-related enquiries:

security@moseyaround.com

For privacy enquiries:

privacy@moseyaround.com

For legal enquiries:

legal@moseyaround.com

For general support:

support@moseyaround.com

## 22. Relationship with Other Documents

This Security Statement forms part of the Mosey Legal Suite and should be read together with the:

- Terms & Conditions
- Privacy Policy
- Fair Play & Anti-Cheat Policy
- Cookie Policy
- Third-Party Services Register

Where another document provides more detailed information about a specific topic, the documents should be read together.

## 23. Final Statement

Protecting our members, partners and platform is a continuous commitment.

We will continue to invest in appropriate technical and organisational measures, review our practices as technology evolves and work with members, partners and security researchers to maintain a secure and trustworthy platform.

No security programme is ever complete, but continuous improvement is at the heart of how Moseyaround Limited approaches security.