Community.OS - Mosa Acceptable Use & Communications Policy

Document	**Mosa Acceptable Use & Communications Policy**
Document Version	v1.0
Reviewed	27th September 2026
Status	Approved
Parent Company	Sidekick Platforms
Platform Brand	Community.OS
Consumer Product	Mosa
Brand Promise	Making Participation Visible
Core Message	When participation becomes visible, communities become stronger.
Supporting Line	Every little bit helps.
Guide	Pitch

Table of Contents

Community.OS - Mosa Acceptable Use & Communications Policy 1
Table of Contents 2
1. About This Policy 4
2. Who This Policy Applies To 4
3. Our Approach 5
4. Use Mosa Lawfully 6
5. Treat People Appropriately 6
6. Exploitation, Coercion and Abuse of Vulnerability 7
7. Threats, Violence and Immediate Safety 7
8. Children and Young People 8
9. Adults Communicating With Young People 8
10. Sexual Exploitation and Grooming 9
11. Harassment, Bullying and Repeated Unwanted Contact 9
12. Discrimination and Inclusion 9
13. Impersonation and Identity Misuse 10
14. Truthful Information, Documents and Credentials 10
15. Fraud, Scams and Deliberate Deception 11
16. Mosa as a Communication Channel 12
17. Different Types of Communication 12
18. Organisation Communications 13
19. Personal One-to-One and Group Conversations 13
20. Group Administration 14
21. Blocking and Restriction 14
22. Spam and Unwanted Communications 15
23. Information and Privacy Misuse 15
24. Scraping and Bulk Extraction 16
25. Security and Platform Integrity 16
26. Circumventing Safeguards 16
27. Content 17
28. Organisation Responsibilities 17
29. Organisation Policies 18
30. Reporting Concerns 18
31. A Report Is Not Automatically a Finding 19
32. False or Abusive Reports 19
33. Organisation Moderation and Platform Moderation 19
34. How Mosa May Respond 20
35. Interim Safety Measures 21
36. Proportionate Response 22
37. Serious Breaches 22

38. Repeated Breaches 23
39. Organisation Restrictions, Suspension and Termination 23
40. Subscription Fees During Organisation Restriction or Suspension 24
41. Evidence and Records 24
42. Moderator Access 24
43. Cooperation With Investigations 25
44. Referral to Organisations 25
45. Referral to Authorities 26
46. Appeals and Review 26
47. Emergency and Protective Action 27
48. Organisation Action Is Separate 27
49. Lawful Reporting and Good-Faith Concerns 27
50. Automated Systems 28
51. Different Communities, Same Foundation 28
52. Changes to This Policy 28
53. Relationship With Our Terms 29
54. Contact and Reporting 29
Our Community Trust Commitment **29**

1. About This Policy

Mosa exists to make participation easier and more visible across the communities people are part of.

Communities contain different people, opinions, relationships, responsibilities and ways of participating. We do not expect everybody to agree with each other.

We do expect people to treat each other appropriately and to use Mosa in ways that support rather than undermine the communities they are part of.

This Acceptable Use & Communications Policy explains the standards that apply when people and Organisations use Mosa and Community.OS.

It also explains what may happen when those standards are not met.

This Policy applies alongside the:

- Mosa Terms of Use;
- Mosa Organisation Terms;
- Mosa Privacy Policy;
- Children & Young People Privacy Notice;
- Mosa Data Processing & Organisation Privacy Terms;
- applicable Organisation policies;
- and other terms or policies that apply to a particular Community Space or capability.

2. Who This Policy Applies To

This Policy applies to people and Organisations using Mosa or Community.OS, including:

- participants;
- parents, guardians and representatives;
- Organisation administrators;
- coaches;
- teachers;
- team managers;
- volunteers;
- committee members;
- employees;
- officials;
- Group administrators;
- Organisation representatives;
- and other authorised users.

Different responsibilities may apply depending on a person's role, authority, relationship and context.

3. Our Approach

Mosa should be a place where people can participate **safely, respectfully and confidently**.

Our approach is built around several important distinctions.

3.1 Disagreement ≠ Abuse

People can disagree.

They can express different views, challenge decisions and participate in robust community discussion.

Disagreement does not itself breach this Policy.

3.2 Organisation Authority ≠ Unlimited Communication Authority

A coach, teacher, administrator or Organisation representative may legitimately need to communicate with people.

Their role does not give them unlimited authority to contact anybody about anything.

3.3 Access to Information ≠ Permission to Repurpose It

Being able to see information for one legitimate reason does not mean it can be copied, exported, published or used for another purpose.

3.4 A Report ≠ A Finding

A report tells us that something may require attention.

It does not automatically establish that misconduct occurred.

3.5 Moderation ≠ Automatic Punishment

Moderation may involve understanding context, reducing immediate risk, investigating what happened and determining an appropriate response.

3.6 Safeguarding Can Override Ordinary Communication Authority

A communication that might otherwise be technically possible may be restricted where safety or safeguarding requires it.

3.7 Personal Conversation ≠ Organisation Communication

A private conversation between participants is different from communication sent using Organisation authority.

That distinction affects:

- responsibility;
- moderation;
- privacy;
- safeguarding;
- and when Sidekick Platforms may intervene.

4. Use Mosa Lawfully

You must not use Mosa or Community.OS to engage in, facilitate or deliberately assist unlawful activity.

This includes using Mosa to facilitate:

- fraud;
- threats or violence;
- unlawful harassment;
- unlawful discrimination;
- exploitation;
- stalking;
- scams;
- theft;
- malicious cyber activity;
- child exploitation;
- sexual exploitation;
- or other unlawful conduct.

Mosa may take action where conduct creates serious safety, legal, security, safeguarding or platform-integrity concerns.

5. Treat People Appropriately

People using Mosa must not use the platform to:

- threaten another Person;
- harass or abuse another Person;
- bully or intimidate;
- deliberately humiliate or degrade another Person;
- engage in unlawful discrimination;
- repeatedly target somebody who has asked for unwanted interaction to stop;
- encourage others to harass or target somebody;
- deliberately expose private information to harm somebody;
- or engage in other seriously harmful behaviour.

Context matters.

A disagreement between committee members is not automatically harassment.

A coach providing reasonable performance feedback is not automatically bullying.

An Organisation enforcing legitimate participation requirements is not automatically discriminatory.

Legitimate authority or disagreement cannot, however, be used as a cover for abusive conduct.

6. Exploitation, Coercion and Abuse of Vulnerability

People must not use Mosa to exploit, coerce or deliberately take advantage of another Person.

This may include:

- sexual exploitation;
- coercion;
- extortion or blackmail;
- financial exploitation;
- abuse of a position of authority or trust;
- deliberately exploiting vulnerability, disability or dependence;
- coercive or controlling behaviour;
- manipulating another Person for unlawful or seriously harmful purposes;
- or deliberately using information or authority to obtain an improper advantage over another Person.

A Person may be particularly vulnerable because of:

- age;
- disability;
- dependency;
- personal circumstances;
- authority relationships;
- or another factor.

Prohibited exploitation is not limited to children or young people.

Where conduct creates a serious safety, safeguarding or legal concern, Mosa may take immediate protective action and may refer the matter to an appropriate authority where permitted or required.

7. Threats, Violence and Immediate Safety

Mosa must not be used to make credible threats of violence or encourage serious harm to another Person.

Where we reasonably believe there may be an immediate risk to somebody's safety, we may take urgent action.

This may include:

- restricting communication;
- restricting or suspending an Account;
- preserving relevant information;
- notifying an appropriate Organisation safeguarding contact;
- or contacting emergency services or another appropriate authority where reasonably necessary or required by law.

Mosa is not an emergency service.

Where somebody is in immediate danger, users should contact the appropriate emergency service directly.

8. Children and Young People

Children and young people require additional care.

A young Person remains their own Person within Mosa even where a parent, guardian, carer or other authorised representative helps manage their participation.

People must not use Mosa to:

- groom or sexually exploit a child or young Person;
- send sexualised or exploitative material to a young Person;
- deliberately circumvent child-safety controls;
- manipulate a young Person into concealing inappropriate communication;
- impersonate a parent, guardian or authorised representative;
- misuse authority over a young Person;
- or engage in other conduct that creates an inappropriate safeguarding risk.

Serious concerns involving children may be escalated beyond ordinary community moderation.

9. Adults Communicating With Young People

An adult's legitimate relationship with a young Person does not automatically create unrestricted direct communication authority.

For example, being a:

- coach;
- teacher;
- team manager;
- Organisation administrator;
- volunteer coordinator;
- official;
- or committee member

does not necessarily permit unrestricted private messaging with a child.

Depending on the context, Mosa or an Organisation may require:

- Group communication;
- parent or representative visibility;
- another authorised adult to be included;
- approval before communication begins;
- restrictions on direct messaging;
- or another safeguarding control.

Users must not deliberately circumvent these controls by moving a protected conversation into another Mosa context.

10. Sexual Exploitation and Grooming

Mosa must not be used to sexually exploit, groom or facilitate the sexual exploitation of another Person.

This prohibition applies to conduct involving adults as well as children, with additional safeguarding protections applying to children and young people.

Prohibited behaviour may include attempts to:

- sexualise interactions with a child;
- solicit sexual material from a child;
- send sexual material to a child;
- build inappropriate secrecy with a child;
- pressure or coerce another Person into sexual activity;
- exploit vulnerability, dependency or a position of authority;
- facilitate sexual exploitation;
- or use Mosa to support other unlawful sexual conduct.

Where appropriate, Mosa may immediately restrict or suspend relevant access while a concern is investigated.

Serious matters may be referred to relevant Organisations, safeguarding bodies, law enforcement or other authorities where appropriate or required.

11. Harassment, Bullying and Repeated Unwanted Contact

People should be able to participate without being repeatedly targeted through Mosa.

Repeated unwanted contact may breach this Policy even where an individual message would not, by itself, be serious enough to constitute misconduct.

People must not use:

- multiple conversations;
- Groups;
- alternate Accounts;
- Organisation communication capabilities;
- invitations;
- or other Mosa features

to deliberately bypass a block or communication restriction.

Legitimate Organisation operational communications may continue through an authorised pathway even where ordinary direct communication between two people has been blocked.

12. Discrimination and Inclusion

Mosa must not be used to engage in unlawful discrimination or unlawful discriminatory conduct.

At the same time, Organisations may legitimately establish participation criteria where those criteria are lawful and appropriate.

Examples may include:

- age groups;
- competition eligibility;
- qualifications;
- safety requirements;
- membership requirements;
- team selection;
- activity capacity;
- or role-specific requirements.

The existence of participation criteria does not itself establish discrimination.

Organisations remain responsible for ensuring their decisions and criteria comply with applicable law.

13. Impersonation and Identity Misuse

You must not deliberately impersonate another Person or falsely claim authority you do not have.

This includes pretending to be:

- another participant;
- a parent or guardian;
- an Organisation administrator;
- a coach;
- an official;
- an employee of Sidekick Platforms;
- or another authorised Person.

Legitimate representation supported by Mosa is not impersonation.

Where one Person acts for another, Mosa should preserve who actually performed the action and the capacity in which they acted.

14. Truthful Information, Documents and Credentials

People must take reasonable care to provide information that is truthful and accurate when that information is used to establish:

- identity;
- representation;
- membership;
- eligibility;
- qualifications;
- licences;
- checks;
- certifications;

- attendance;
- participation;
- authority;
- payment entitlement;
- or another consequential status.

You must not knowingly:

- provide materially false information;
- forge, alter or fabricate a document;
- upload somebody else's credential as your own;
- manipulate an expiry date or qualification status;
- falsely claim a role, relationship or authority;
- falsify participation or attendance;
- misrepresent eligibility;
- deliberately provide misleading evidence;
- or use false information to obtain access, participation, benefits or authority you would not otherwise receive.

An innocent mistake, outdated information or genuine disagreement about a record is not automatically misconduct.

Where Mosa reasonably suspects that consequential information or evidence has been falsified, we may:

- restrict reliance on that information;
- request further information or verification;
- identify the information as disputed or unverified;
- notify an appropriately authorised Organisation where relevant;
- preserve relevant evidence;
- restrict affected capabilities;
- or take another proportionate action.

Serious or deliberate falsification may result in suspension or termination.

15. Fraud, Scams and Deliberate Deception

Mosa must not be used to:

- conduct fraud;
- solicit money deceptively;
- operate scams;
- misrepresent an Organisation;
- deliberately falsify consequential records;
- manipulate payments;
- misrepresent authority;
- or deliberately deceive another Person in a way likely to cause material harm.

Ordinary mistakes, disputed records or good-faith disagreements are not automatically fraud.

16. Mosa as a Communication Channel

Mosa may provide Organisations and participants with convenient ways to communicate.

It does not replace every other form of communication.

Depending on the circumstances, people and Organisations may still need to use:

- telephone;
- SMS;
- email;
- emergency services;
- official Organisation channels;
- governing-body channels;
- or another appropriate communication method.

Mosa should not be relied upon as the sole method for urgent, emergency, medical, safeguarding or other time-critical communication unless the relevant Organisation has expressly established an appropriate process for that purpose.

Delivery of a Mosa message, notification or announcement does not automatically establish that the recipient has seen, understood or acted upon it.

Mosa is not an emergency service.

Where somebody is in immediate danger or urgent assistance is required, contact the appropriate emergency service or other appropriate authority directly.

17. Different Types of Communication

Mosa may support different communication modes, including:

- operational Organisation communications;
- announcements;
- activity or Opportunity communications;
- Organisation-created Groups;
- participant-created Groups;
- one-to-one participant conversations;
- notifications;
- and other supported communication types.

These communication modes do not necessarily have identical:

- authority;
- privacy;
- moderation;
- safeguarding;
- retention;
- or participant-control rules.

The distinction between Organisation communications and participant conversations is intentional.

18. Organisation Communications

Organisations may use Community.OS to communicate with people where there is a legitimate relationship and purpose.

Organisation communication authority should remain connected to that context.

For example:

Coach of U12 Rams → team operational communication

does not automatically become:

Coach → unrestricted personal messaging with every family member

Organisation administrators and representatives must not misuse Organisation communication capabilities for unrelated personal, commercial or inappropriate purposes.

Using an Organisation account, administrator capability, official Group, Opportunity, Activity or other Organisation-controlled context creates a greater expectation that the communication is being made legitimately on behalf of, or within the authority of, that Organisation.

Misuse of that authority may result in action by the Organisation, Mosa or both.

19. Personal One-to-One and Group Conversations

Mosa may support personal one-to-one conversations and participant-created Group conversations that are not controlled, endorsed or operated by an Organisation.

These conversations are different from:

- official Organisation communications;
- Organisation-created Groups;
- communications sent using Organisation authority;
- activity or Opportunity communications;
- safeguarding communications;
- and other operational communications.

People remain responsible for how they communicate with each other.

Sidekick Platforms does not ordinarily intend to monitor, adjudicate or intervene in ordinary personal disagreements, interpersonal conflict, rudeness or disputes occurring within private participant conversations merely because Mosa was used as the communication channel.

Where appropriate, participants should generally use available controls such as:

Mute → Leave → Block → Report

depending on the circumstances.

Platform intervention in personal conversations should generally be reserved for circumstances involving significant platform, safety or legal concerns, such as:

- credible threats;
- serious harassment;
- stalking;
- exploitation;
- child safeguarding;
- serious fraud;
- impersonation creating material harm;
- unlawful content;
- security threats;
- deliberate evasion of platform safety controls;
- or serious or repeated conduct creating material risk to people or Community.OS.

A rude message, argument, friendship breakdown, difference of opinion or ordinary interpersonal dispute will not necessarily result in Mosa taking platform action.

20. Group Administration

Participant-created Groups may support Group administrators.

A Group administrator may have authority to:

- manage membership;
- establish reasonable Group rules;
- invite or remove participants;
- manage available Group settings;
- moderate the Group;
- or manage other supported Group capabilities.

Group administration does not create broader authority over participants':

- identities;
- Households;
- Organisation relationships;
- private information;
- or Community Story.

An Organisation-created or Organisation-controlled Group may have additional rules because it forms part of the Organisation's operational context.

21. Blocking and Restriction

Mosa may provide controls allowing people to:

- block another Person;
- restrict interactions;

- leave a conversation;
- mute notifications;
- report conduct;
- or otherwise reduce unwanted communication.

People must not deliberately circumvent another Person's legitimate block or restriction.

Blocking another Person does not necessarily prevent legitimate operational or safety communications being delivered through an authorised Organisation pathway.

22. Spam and Unwanted Communications

Mosa must not be used to send spam or systematically distribute irrelevant or inappropriate communications.

Organisations may legitimately communicate with people about matters arising from their relationship, including:

- membership;
- registrations;
- events;
- rosters;
- activities;
- safety;
- requirements;
- participation;
- and Organisation operations.

Commercial and marketing communications may be subject to additional consent, preference and legal requirements.

An Organisation relationship does not create unlimited marketing permission.

23. Information and Privacy Misuse

You must not misuse personal information available through Mosa.

This includes deliberately:

- collecting information without a legitimate reason;
- accessing information outside your authority;
- copying participant information for an unrelated purpose;
- publishing private information without authority;
- exporting information to circumvent Mosa privacy controls;
- using participant information for unauthorised marketing;
- attempting to discover information hidden by privacy controls;
- or using information to harass, exploit or harm somebody.

Information access remains subject to the purpose and authority that justified it.

24. Scraping and Bulk Extraction

Unless expressly authorised, you must not use:

- scraping;
- automated extraction;
- bots;
- scripts;
- crawlers;
- bulk-download mechanisms;
- unauthorised APIs;
- or similar techniques

to systematically collect information from Mosa or Community.OS.

Authorised exports, integrations and APIs remain subject to their applicable permissions and purposes.

25. Security and Platform Integrity

You must not attempt to compromise Community.OS or another user's security.

This includes attempting to:

- gain unauthorised access;
- bypass authentication;
- circumvent permissions;
- exploit vulnerabilities;
- obtain another Person's credentials;
- interfere with security controls;
- introduce malicious code;
- disrupt service availability;
- manipulate audit records;
- interfere with monitoring;
- abuse APIs;
- evade rate limits or technical controls;
- or deliberately facilitate another Person doing these things.

Legitimate security research must be conducted through any responsible disclosure process we make available and must not unnecessarily compromise participant information or service availability.

26. Circumventing Safeguards

You must not deliberately bypass controls intended to protect:

- children;
- young people;
- other vulnerable participants;
- participant privacy;
- sensitive information;

- communication safety;
- Account security;
- Organisation authority;
- or platform integrity.

Attempting to reproduce a prohibited interaction through another Mosa capability may itself constitute a breach.

27. Content

You are responsible for content you intentionally provide through Mosa, subject to the Mosa Terms of Use and Organisation Terms.

Content must not be used to distribute material that is:

- unlawful;
- fraudulent;
- malicious;
- exploitative;
- seriously abusive;
- deliberately deceptive in a materially harmful way;
- or otherwise prohibited by this Policy.

Content or evidence supplied to establish identity, eligibility, qualification, authority or another consequential status must also comply with Section 14.

Context matters when assessing content.

Material may sometimes be legitimately retained or shared for:

- reporting;
- safeguarding;
- evidence;
- education;
- moderation;
- investigation;
- or another lawful purpose

even where the underlying conduct depicted in that material would itself be prohibited.

28. Organisation Responsibilities

Organisations play an important role in maintaining safe communities.

An Organisation should take reasonable steps to:

- appoint appropriate administrators;
- manage permissions;
- periodically review privileged access;
- maintain appropriate safeguarding practices;

- respond to concerns within its responsibility;
- protect participant information;
- manage Organisation Groups appropriately;
- use communication authority appropriately;
- and remove authority that is no longer required.

An Organisation should not knowingly allow its administrators or representatives to misuse Community.OS.

Repeated failure to appropriately address serious misuse within the Organisation's control may itself become relevant to Mosa's relationship with the Organisation.

29. Organisation Policies

An Organisation may establish its own:

- codes of conduct;
- communication policies;
- safeguarding policies;
- team rules;
- membership rules;
- or other legitimate requirements.

Those policies may impose stronger behavioural or safeguarding requirements within the Organisation's context.

They cannot authorise conduct prohibited by:

- law;
- mandatory Mosa safeguards;
- the Mosa Organisation Terms;
- or this Policy.

30. Reporting Concerns

Mosa should make it reasonably straightforward for people to report concerns.

Depending on available functionality, concerns may include:

- messages;
- conversations;
- participants;
- Groups;
- content;
- harassment;
- spam;
- impersonation;
- safeguarding concerns;
- threats;
- fraud;
- privacy misuse;

- security concerns;
- or other inappropriate behaviour.

People may also contact us directly where appropriate.

Reporting a personal conversation does not necessarily mean Mosa will adjudicate an ordinary interpersonal dispute.

31. A Report Is Not Automatically a Finding

Submitting a report does not automatically establish that another Person or Organisation breached this Policy.

Where appropriate, we may consider:

- what was reported;
- available evidence;
- relevant context;
- seriousness;
- previous related behaviour;
- safeguarding implications;
- Organisation information;
- whether Organisation authority was being exercised;
- whether the matter is primarily an interpersonal dispute;
- and other relevant circumstances.

32. False or Abusive Reports

Reporting tools must not be used to:

- harass another Person;
- retaliate against somebody;
- deliberately make false allegations;
- overwhelm moderators;
- coordinate malicious reporting;
- or manipulate Organisation or platform processes.

A report made honestly does not breach this Policy merely because the concern is ultimately not substantiated.

Deliberate or repeated misuse of reporting mechanisms may itself result in action.

33. Organisation Moderation and Platform Moderation

Mosa distinguishes between:

Organisation Moderation

Moderation arising from an Organisation's legitimate authority over its own:

- activities;
- Groups;
- membership;
- representatives;
- Opportunities;
- communications;
- or community context.

Platform Moderation

Action taken by Sidekick Platforms to protect:

- Mosa;
- Community.OS;
- participants;
- safety;
- safeguarding;
- security;
- privacy;
- or platform integrity.

These responsibilities may overlap.

They are not interchangeable.

An Organisation may take action under its own rules independently of whether Sidekick Platforms takes platform-level action.

Likewise, Sidekick Platforms may take platform action where appropriate even if an Organisation chooses not to act.

For ordinary personal one-to-one and participant-created Group conversations, Sidekick Platforms generally intends platform moderation to remain limited to circumstances where the conduct creates a sufficiently significant safety, safeguarding, legal, security or platform-integrity concern.

34. How Mosa May Respond

Where we reasonably believe this Policy, our Terms or applicable law may have been breached, we may take action appropriate to the circumstances.

Depending on the nature and seriousness of the matter, action may include:

- taking no platform action where the matter is more appropriately managed between participants or by an Organisation;
- providing a warning;
- requesting that behaviour stop;
- removing or limiting content where we have appropriate authority to do so;
- limiting communication capability;
- preventing new conversations;
- restricting contact with particular people;
- removing somebody from a Group;

- limiting particular features;
- restricting Organisation capabilities;
- requiring additional verification;
- temporarily restricting an Account;
- suspending an Account;
- temporarily suspending an Organisation;
- permanently restricting particular capabilities;
- terminating a Person's or Organisation's access;
- preserving relevant evidence;
- referring a matter to an Organisation or safeguarding contact;
- reporting or referring a matter to an appropriate authority where necessary or required;
- or taking another reasonable protective action.

We do not need to use these responses in a fixed sequence.

A serious incident may justify immediate restriction or suspension without a prior warning.

35. Interim Safety Measures

Sometimes we may need to act before an investigation or review is complete.

Where there is a credible concern involving:

- immediate safety;
- children;
- vulnerable participants;
- safeguarding;
- serious harassment;
- exploitation;
- serious privacy misuse;
- fraud;
- Account compromise;
- security;
- or platform integrity,

we may apply an interim restriction.

An interim measure may include:

- restricting communication;
- restricting contact with a particular Person;
- removing somebody from a Group;
- limiting an Account;
- suspending message initiation;
- restricting access to particular information;
- restricting an Organisation capability;
- temporarily suspending an Account;
- or temporarily suspending an Organisation.

An interim safety measure is **not necessarily a final finding that misconduct occurred**.

36. Proportionate Response

Where practical and appropriate, our response should be proportionate to the risk and conduct involved.

Relevant factors may include:

- seriousness;
- actual or potential harm;
- whether children or vulnerable participants are involved;
- whether Organisation authority was being exercised;
- whether conduct was intentional;
- repetition;
- previous warnings or restrictions;
- attempts to evade controls;
- cooperation;
- immediate risk;
- legal requirements;
- whether the conduct occurred in an ordinary personal conversation;
- and whether a narrower restriction can adequately address the concern.

A problem in one Organisation or communication context does not automatically require a Person to lose every unrelated Mosa capability.

However, serious, repeated or platform-wide abuse may justify broader action.

37. Serious Breaches

Some conduct may justify immediate or significant action.

Examples may include:

- child sexual exploitation or grooming;
- serious sexual or financial exploitation of another Person;
- credible threats of serious violence;
- serious fraud;
- deliberate compromise of another Person's Account;
- malicious attacks against Community.OS;
- deliberate exposure of highly sensitive information;
- serious stalking or harassment;
- serious coercion or extortion;
- deliberate falsification of consequential credentials or evidence;
- repeated attempts to evade safeguarding restrictions;
- or other conduct creating substantial risk to people, Organisations or the platform.

Depending on the circumstances, Mosa may act immediately to protect participants or Community.OS.

38. Repeated Breaches

Repeated lower-level misconduct may become serious when considered together.

For example:

Repeated unwanted messages after warnings

may justify stronger action than an isolated inappropriate message.

Likewise:

Repeated Organisation misuse after warnings or remediation requirements

may justify broader Organisation restrictions or suspension.

Attempts to evade previous restrictions may also result in stronger action.

39. Organisation Restrictions, Suspension and Termination

An Organisation may be subject to action under this Policy where conduct by the Organisation, or people acting through its authority, creates a material concern.

Depending on severity, frequency and risk, we may:

Restrict a capability → Temporarily suspend a capability → Temporarily suspend the Organisation → Require remediation → Permanently restrict a capability → Terminate the Organisation's access

We may act immediately where reasonably necessary to address serious:

- safety;
- safeguarding;
- privacy;
- fraud;
- security;
- legal;
- or platform-integrity risk.

Where appropriate, we may require an Organisation to take remedial action before access or capabilities are restored.

This may include:

- removing administrator access;
- changing permissions;
- addressing inappropriate communications;
- improving safeguarding controls;
- correcting misleading content;
- securing compromised credentials;
- or taking another reasonable corrective action.

Suspension may be temporary or may continue until specified remediation requirements are satisfied.

Serious conduct, repeated violations or circumstances that cannot reasonably be remedied may result in permanent restriction or termination.

40. Subscription Fees During Organisation Restriction or Suspension

Where an Organisation is restricted or suspended because of its breach, misconduct, misuse or failure to comply with applicable requirements, that restriction or suspension does not automatically:

- extend the Organisation's subscription period;
- pause applicable subscription fees;
- create a service credit;
- create a partial refund;
- or create a refund for unused subscription time.

Any refund, credit or other adjustment remains subject to:

- the Mosa Organisation Terms;
- applicable commercial terms;
- the circumstances giving rise to the restriction;
- and rights that cannot lawfully be excluded.

Nothing in this section removes any refund or other right that an Organisation has under applicable law.

41. Evidence and Records

Where a report concerns serious misconduct, safeguarding, security, fraud or another significant issue, Mosa may preserve relevant information where appropriate.

This may include information that would otherwise have been removed because somebody:

- deleted a message;
- left a conversation;
- blocked another Person;
- closed an Account;
- or attempted to remove relevant content.

Retention should remain connected to a legitimate purpose.

42. Moderator Access

Investigating a report does not give a moderator unrestricted access to everything Mosa knows about the people involved.

Access should remain limited to what is reasonably necessary for the relevant:

- moderation;

- safety;
- security;
- fraud;
- or safeguarding purpose.

Where participant communications use stronger cryptographic protections, reporting may require the reporting participant to deliberately provide the reported content and appropriate surrounding context rather than creating permanent platform access to every conversation.

43. Cooperation With Investigations

Where reasonably required, users and Organisations may be asked to cooperate with an investigation involving:

- safety;
- safeguarding;
- security;
- fraud;
- privacy misuse;
- serious falsification;
- or another serious breach of this Policy.

People and Organisations must not deliberately:

- destroy relevant evidence;
- falsify information;
- impersonate another Person;
- interfere with an investigation;
- retaliate against a reporter;
- or attempt to bypass an interim restriction.

44. Referral to Organisations

Some concerns are primarily matters for the relevant Organisation.

For example, an Organisation may be responsible for:

- coach conduct;
- team behaviour;
- membership discipline;
- volunteer conduct;
- employee behaviour;
- activity management;
- Organisation communications;
- or Organisation-specific codes of conduct.

Where appropriate, Mosa may refer or provide relevant information about a concern to an authorised Organisation representative.

Any disclosure should remain consistent with applicable privacy, safeguarding and legal requirements.

We will not ordinarily refer every private disagreement between participants to an Organisation merely because those participants happen to belong to the same Organisation.

45. Referral to Authorities

There may be circumstances where information is referred to:

- police;
- emergency services;
- child protection authorities;
- regulators;
- courts;
- governing bodies;
- or another appropriate authority.

This may occur where:

- required by law;
- responding to valid legal process;
- necessary to address a serious safety or safeguarding concern;
- or otherwise permitted by applicable law.

Nothing in this Policy means Mosa undertakes to report every dispute or alleged breach to an external authority.

46. Appeals and Review

Where appropriate, Mosa may provide a way for a Person or Organisation to request review of a significant platform moderation decision.

The available review process may depend on:

- the nature of the decision;
- seriousness;
- safeguarding requirements;
- legal restrictions;
- security;
- privacy;
- and whether disclosure of particular information could create additional harm.

A review does not necessarily require Mosa to disclose:

- another Person's confidential information;
- safeguarding information;
- security-sensitive information;
- internal detection methods;
- or information we are legally restricted from disclosing.

47. Emergency and Protective Action

Nothing in this Policy prevents Mosa from taking immediate reasonable action where delay could materially increase risk to:

- a Person;
- a child or young Person;
- another vulnerable participant;
- an Organisation;
- participant information;
- Community.OS;
- or another party.

Protective action may occur before ordinary review processes are complete.

48. Organisation Action Is Separate

An Organisation may independently take action under:

- its membership rules;
- employment arrangements;
- codes of conduct;
- safeguarding obligations;
- sporting rules;
- school policies;
- or other legitimate authority.

Mosa does not determine every Organisation disciplinary matter merely because the relevant people use Community.OS.

Likewise:

No platform breach found ≠ Organisation must take no action

and:

Organisation takes no action ≠ Mosa cannot take platform action

49. Lawful Reporting and Good-Faith Concerns

Nothing in this Policy is intended to prevent a Person from:

- making a lawful complaint;
- raising a genuine safeguarding concern;
- reporting suspected wrongdoing;
- contacting a regulator;
- contacting law enforcement;
- obtaining legal advice;

- or exercising another legal right.

A Person will not breach this Policy merely because they raise a concern in good faith.

50. Automated Systems

Mosa may use automated systems to assist with:

- spam detection;
- security;
- abuse detection;
- suspicious activity;
- rate limiting;
- safeguarding workflows;
- fraud detection;
- or moderation triage.

Automated signals do not necessarily establish misconduct.

Significant action should remain subject to appropriate governance according to the nature and consequence of the decision.

51. Different Communities, Same Foundation

Community.OS may support many different Community Spaces and Organisations.

A school, sporting club, charity, community group and neighbourhood may require different operational rules.

Those differences do not create separate fundamental standards for:

- safety;
- privacy;
- safeguarding;
- security;
- or appropriate platform use.

New Community Spaces inherit this foundation.

52. Changes to This Policy

We may update this Policy as:

- Mosa develops;
- Community.OS introduces new capabilities;
- communication features evolve;
- safeguarding practices develop;
- applicable law changes;
- or we learn from real community use.

Material changes may be communicated through Mosa or another appropriate channel.

The current version and last-updated date will be identified.

Where appropriate, historical versions may be retained.

53. Relationship With Our Terms

A breach of this Policy may also constitute a breach of:

- the Mosa Terms of Use;
- the Mosa Organisation Terms;
- another applicable agreement;
- or applicable law.

Where those Terms permit us to restrict, suspend or terminate access, a breach of this Policy may form the basis for that action.

Nothing in this Policy limits rights or obligations that cannot lawfully be limited.

54. Contact and Reporting

Mosa and Community.OS are operated by:

OSA Management Pty Ltd
ABN 62 677 945 863
Trading as Sidekick Platforms

For general concerns or questions:

hello@oncommunityos.com

As Mosa develops, we may provide dedicated in-product reporting, safety, safeguarding and security reporting pathways.

Our Community Trust Commitment

Mosa exists to help people participate in communities, not to make communities sterile or disagreement impossible.

People will disagree.

Teams will have difficult conversations.

Committees will make unpopular decisions.

Coaches will provide feedback.

Friends will argue.

Group chats will sometimes get messy.

Organisations will enforce legitimate rules.

Participants will sometimes make mistakes.

None of those things automatically means trust has been broken.

Mosa may become an important way people communicate with the communities and people around them. We want people to be able to use it confidently for genuine everyday communication without assuming Sidekick Platforms is watching, judging or refereeing every conversation.

At the same time, providing a communication platform does not mean ignoring serious harm.

What matters is the context, the authority being exercised, the seriousness of the conduct and the risk created.

Our expectation is simple:

> **Participate honestly. Treat people appropriately. Respect boundaries. Protect people who need additional care. Use information for the reason you were trusted with it. Don't deliberately undermine the systems designed to keep people safe.**

For ordinary personal conversations, people should generally remain in control of their own relationships and use tools such as muting, leaving and blocking where appropriate.

Where somebody is acting through an Organisation, exercising trusted authority or using Mosa's operational capabilities, greater responsibility comes with that authority.

Where safety, safeguarding, serious exploitation, fraud, security, illegality or serious platform abuse is involved, Mosa may intervene.

When something goes wrong, our response should reflect context and consequence.

A minor mistake should not automatically become a platform ban.

A rude message should not automatically become a moderation case.

A report should not automatically become a finding.

An Organisation should have an opportunity to remedy problems where that is reasonable and safe.

But serious misconduct should not be hidden behind procedural complexity either.

Where trust is seriously or repeatedly breached, **Mosa may restrict capabilities, preserve evidence, temporarily or permanently suspend access, terminate access and escalate the matter where appropriate to protect people, Organisations and the wider community.**

The aim is not punishment for its own sake.

It is to preserve a platform where people can participate and communicate with confidence.