Guidance

# Acceptable Use Policy

Updated 15 November 2026

NM Group

## 1. Purpose and scope

This Acceptable Use Policy sets out the standards of behaviour and security required when using NM Group's information, systems, services and equipment. Its purpose is to support legitimate activities while protecting users, maintaining reliable services and preventing unauthorised access, misuse or disclosure of information.

This policy applies to all users of NM Group resources, including administrators, employees, contractors, collaborators, volunteers, customers and visitors, where applicable. It covers accounts, devices, networks, applications, websites, communications services, storage, development environments and security equipment. It applies to remote access and to personally owned devices when they are used to access NM Group resources or handle information on its behalf.

## 2. Authorised use and individual responsibility

Users must use NM Group resources lawfully, responsibly and within the authority given to them. Authorisation may arise from an assigned role, an agreed project, the intended functionality of a service or specific permission from an authorised system owner. Being able to access information or perform an action does not, by itself, establish permission to do so.

Users must follow the security requirements and reasonable operating instructions provided for the systems they use. They must not use another person's account, exceed their assigned permissions or attempt to bypass a restriction. Access to one NM Group service, including through a shared sign-in account, does not automatically authorise access to other services or administrative functions.

## 3. Accounts and authentication

Users must protect their accounts and authentication credentials against loss, disclosure and unauthorised use. Passwords must be strong and must not be reused for unrelated services. Required authentication measures, including multi-factor authentication, must remain enabled. Users must not share personal passwords, recovery codes, security tokens or authentication prompts, or approve a sign-in request they did not initiate.

Shared, service and test accounts may be used only for an approved purpose and must have a responsible owner. Administrative access must be used only for authorised tasks. Users must report suspected account compromise promptly and notify the relevant administrator when access is no longer required. Administrators must review permissions when responsibilities change and remove access that is no longer justified.

## 4. Protecting information

Information must be accessed, collected, used and disclosed only for an authorised and lawful purpose. Users must handle information according to its sensitivity, limit access to those who require it and check recipients and permissions before sharing. Personal information, private communications, confidential project material and security details must not be accessed out of curiosity or used to further personal interests.

Information must be stored, transferred and disposed of using appropriate methods. Users must not place confidential information in personal email accounts, public links, unapproved storage services or public repositories. Retention and preservation requirements must be followed, including instructions relating to an investigation or legal obligation. Requests concerning an individual's personal information must be referred to the responsible administrator.

## 5. Conduct and communications

Users must communicate respectfully and must not use NM Group resources for harassment, bullying, threats, unlawful discrimination, exploitation, fraud or impersonation. Creating or distributing unlawful

material, non-consensual intimate imagery, malicious communications or another person's private information without a lawful purpose is prohibited. Users must also respect copyright, software licences and other rights in the material they use.

Communications must not falsely suggest that the sender is authorised to speak for NM Group or another organisation. Users must take care when opening attachments, following links and responding to unexpected requests for information or access. Nothing in this policy prevents lawful criticism, a good-faith complaint, a protected disclosure or reporting concerns to an appropriate authority.

## 6. Devices, software and networks

Users must take reasonable care of equipment, lock unattended devices and maintain the security controls required for their access. Updates, protective software, encryption and logging must not be disabled or bypassed without appropriate authorisation. Software must be lawfully obtained and suitable for the environment in which it is used.

Users may install software, run scripts and change settings where those activities fall within their assigned authority. Additional permission is required before exceeding that authority, exposing internal services or connecting equipment that could compromise shared systems. Unapproved remote-access tools, concealed accounts and connections designed to evade security restrictions are prohibited.

## 7. Remote access and personal devices

Remote access must use the methods approved for the relevant service. Users must take reasonable precautions against unauthorised viewing, overhearing or use of their sessions, particularly in public or shared locations. Confidential information must not be left accessible to other people using the same device.

Personal devices may be used only where permitted and must meet the security requirements applicable to their access. Any management, inspection or removal of NM Group information must have a defined scope and be explained to the user. Permission to connect a personal device does not give NM Group unrestricted access to unrelated personal information.

## 8. Personal use and shared resources

Reasonable incidental personal use is permitted where the service allows it, provided it remains lawful and does not interfere with responsibilities, security or other users. Personal activity must not create unreasonable costs, consume capacity needed for authorised work or imply endorsement by NM Group.

Users must observe applicable storage limits, request limits and other resource controls. They must not deliberately overload systems, interfere with another user's access or use NM Group infrastructure to attack other services. Activities such as reselling access, operating public relays or cryptocurrency mining require specific authorisation unless they are an expressly intended use of the service.

## 9. Development, testing and automation

Development and experimentation are permitted within the environments and responsibilities assigned to the user. Code, configuration and automated processes must be checked appropriately before being introduced into shared or live systems. Credentials must not be included in source code, public repositories or ordinary documentation, and testing must be separated from operational services where necessary to prevent harm.

Security testing requires express authorisation defining the permitted systems, activities and limits. This may include standing permission for recurring checks. Users must remain within that scope and stop if testing creates unexpected disruption or exposes information outside their authority. Permission to test NM Group systems does not extend to third-party systems. Suspected vulnerabilities must be reported without accessing additional records or accounts to demonstrate the issue.

10. Artificial intelligence and external services

External services, including AI tools, may receive only information they are approved to process. Users must not submit confidential material, personal information, credentials or unpublished security details unless the service and the intended use are authorised and lawful. Connecting an integration or automated agent must not grant access beyond what is needed for its purpose.

Users remain responsible for checking generated content and automated actions before relying on or publishing them. Appropriate checks must address accuracy, security, confidentiality, licensing and potential effects on others. Automated tools must not make consequential decisions about individuals unless the process has been specifically authorised and includes appropriate safeguards and oversight.

11. Demonstrations and simulated services

Demonstration, training and simulated environments must be used within their stated purpose and limitations. Synthetic information must be used by default. Real personal information or sensitive operational records must not be introduced unless the environment and processing have been expressly approved and suitably protected.

Users must not present simulated transactions, balances, cards, credentials or records as evidence of real funds, official status or entitlement. Simulated banking and payment workflows must not be used to accept or transfer real money. Demonstrations must make their status clear where someone could otherwise be misled, and must not imply regulatory approval, accreditation or affiliation that has not been established.

12. Physical access and security equipment

Access cards, keys, readers, cameras and other security equipment must be used only for authorised purposes. Personally assigned credentials must not be lent, copied or used to admit an unauthorised person. Users must not interfere with locks, alarms or other protective equipment.

CCTV footage, recordings and access logs may be viewed or disclosed only where necessary for an authorised task. They must not be used for personal surveillance or curiosity. Lost credentials, faults and suspected misuse must be reported promptly. Emergency evacuation and immediate safety needs take priority over routine access restrictions.

13. Monitoring and privacy

NM Group may use security, access and operational records to maintain services, protect accounts, investigate incidents and assess compliance with this policy. The monitoring undertaken will depend on the service and its configuration. Monitoring must have a defined lawful purpose and be necessary and proportionate to that purpose.

Access to monitoring records and stored content must be restricted to authorised people with a legitimate need. Relevant privacy information must explain the monitoring actually undertaken, how information is used and how long it is retained. Administrative access does not permit unrestricted inspection of users' information, and acknowledgement of this policy does not constitute blanket consent to monitoring.

14. Reporting incidents and concerns

Users must report suspected security incidents, accidental disclosures, lost devices, compromised credentials, harmful conduct and other significant concerns as soon as they become aware of them. Reports should be made to NM Group Administration through info@namedmason.com and should describe the affected service, what occurred and any immediate action taken.

Users must not delay reporting while attempting to prove an incident or carry out an unauthorised investigation. Relevant information should be preserved where safe, without collecting unnecessary personal data or redistributing illegal material. Accidental receipt of prohibited content is not itself a

breach; users must stop interacting with it and report the circumstances. Concerns raised in good faith must be handled fairly and without retaliation.

15. Breaches and restrictions

NM Group may take proportionate action where this policy is breached or a credible security or safety risk exists. Action may include guidance, corrective measures, removal of harmful content, restriction of permissions, suspension or withdrawal of access. Immediate protective action may be necessary before an investigation is complete.

Decisions must take account of the evidence, seriousness, impact and relevant circumstances. Restrictions should be limited to the affected service where practical, although wider action may be necessary where a shared account creates risk across several systems. Users will normally be informed of the reason for action and may request a review through NM Group Administration. Any employment, contractual or legal consequences must follow the applicable process.

16. Exceptions and review

Exceptions to this policy must be approved by someone authorised to accept the relevant risk and must identify their scope, duration and safeguards. An exception cannot override applicable law, another person's rights or a third party's authority.

NM Group Administration is responsible for maintaining this policy and reviewing it at least annually and following significant changes to services or risks. Revised versions must identify their effective date and be made available to affected users. Significant changes will be communicated with reasonable notice where practical, and users may be asked to acknowledge the updated requirements.