

Digital Communications & Social Media Policy

OHI Group Corporate Policy

Document Control	
Security Level	Public
Company	OHI Group
Department	CEO Office
Approved By	CEO
Date	July 2026
Revision	1.0

Contents

Digital Communications & Social Media Policy	1
OHI Group Corporate Policy	1
1. Introduction	3
2. Scope	3
3. Definitions	4
4. Core Principles	4
5. Employee Advocacy	5
6. DO's and Don'ts	5
7. Business, Client and Operational Content	6
8. Official and Personal Use	7
9. Media Enquiries	8
10. Confidentiality and Legal Compliance	8
11. Crisis and Issue Management	9
12. Think Before You Post	9
13. Monitoring	9
14. Artificial Intelligence (AI) and Digital Content	10
15. Internal Digital Platforms	10
16. Alignment with OHI Group Values	11
17. Further Guidance and Training	11

1. Introduction

Social media and digital communication platforms are powerful tools for professional networking, brand building, thought leadership, employee advocacy, stakeholder engagement, recruitment, and business development.

They enable OHI Group and its operating entities to engage with customers, clients, partners, suppliers, employees, prospective talent, industry stakeholders, and the wider community. Used responsibly, digital platforms provide opportunities to share knowledge, celebrate achievements, demonstrate expertise, and strengthen relationships.

However, these platforms also present risks to personal and corporate reputation if they are not used appropriately. Content shared online can reach large audiences instantly, may be difficult to remove, and can remain publicly accessible indefinitely.

This Digital Communications & Social Media Policy provides guidance on the responsible use of social media and digital communication platforms by employees, workers, and third parties working for or on behalf of OHI Group and its operating entities.

The purpose of this Policy is to protect the reputation, interests, brands, confidential information, and stakeholder relationships of OHI Group, while encouraging positive, professional, and responsible digital engagement.

Compliance with this Policy is mandatory. This Policy does not form part of an employee's contract of employment and may be amended from time to time. Breaches of this Policy may result in disciplinary action, up to and including termination of employment or cessation of business relationships, where appropriate.

This Policy should be read in conjunction with the OHI Group Code of Ethics and Business Conduct, Information Security Policy, Data Protection and Privacy Policy, AI Policy, Employee Handbook, and other applicable corporate policies and standards.

2. Scope

This Policy applies to:

All employees of OHI Group and its operating entities;
Temporary employees, agency workers, secondees, and other workers performing services for OHI Group;
Consultants and contractors;
Suppliers, service providers, and business partners;
Any third party acting for, representing, or communicating on behalf of OHI Group.

This Policy applies to both business and personal use of social media and digital communication platforms where an individual may be identified as being associated with OHI Group, any of its operating entities, brands, or activities.

It applies across all locations and sectors in which OHI Group operates.

This Policy covers all current and future digital platforms, including but not limited to:

- LinkedIn;
- X (formerly Twitter);
- Facebook;
- Instagram;
- TikTok;
- YouTube;
- Threads;
- WhatsApp;
- Telegram;
- Blogs;
- Forums;
- Discussion boards;
- Podcasts;
- Online communities;
- Collaboration platforms; and
- Any emerging digital communication platform.

Individual operating entities may issue supplementary guidance, as required, to address sector-specific, customer-specific, regulatory, contractual, or operational requirements, provided that such guidance remains consistent with this Group Policy.

3. Definitions

Social Media

Any online platform, website, application, forum, messaging service, or digital channel that enables users to create, share, comment on, publish, or exchange content.

Digital Communications

Electronic communications including social media platforms, blogs, podcasts, online forums, messaging applications, collaboration platforms, websites, and emerging digital technologies.

Official Company Account

Any social media, digital communication, or online platform account created, managed, or authorised by OHI Group or any of its operating entities for business purposes.

Personal Account

Any social media or digital communication account created and managed by an individual for personal or professional use that is not an official company account.

Employee

An individual directly employed by OHI Group or one of its operating entities.

Worker

Any individual performing work or services for OHI Group, including employees, temporary workers, agency workers, subcontracted personnel, consultants, and other individuals engaged through employment or contractual arrangements.

Third Party

Any external organisation or individual acting for, representing, supplying, advising, or providing services to OHI Group, including suppliers, service providers, consultants, agents, distributors, intermediaries, and business partners.

4. Core Principles

When using social media and digital communication platforms, employees and third parties are expected to follow these principles:

Transparency

Be honest about your affiliation with OHI Group or the relevant operating entity where appropriate.

Professionalism

Conduct yourself professionally and in a manner consistent with OHI Group's values, reputation, and standards of behaviour.

Confidentiality

Protect confidential, commercially sensitive, personal, customer, client, and proprietary information at all times.

Respect

Treat colleagues, customers, clients, suppliers, partners, competitors, and members of the public with courtesy, dignity, and professionalism.

Brand Protection

Safeguard the reputation of OHI Group, its operating entities, brands, customers, clients, partners, suppliers, and stakeholders.

Accountability

Take personal responsibility for content you publish, share, endorse, or engage with online.

Accuracy

Ensure information shared publicly is accurate, appropriate, and does not create misunderstanding or misrepresentation.

Responsible Digital Behaviour

Recognise that online activity can impact colleagues, customers, business relationships, and the reputation of OHI Group.

5. Employee Advocacy

OHI Group encourages employees to be positive ambassadors for the organisation.

Sharing approved company content, celebrating achievements, recognising the contributions of colleagues, promoting career opportunities, and participating in professional discussions helps strengthen OHI Group's reputation and demonstrate the expertise and capability of our people.

Employee advocacy supports:

- Brand awareness and reputation;
- Recruitment and talent attraction;
- Industry leadership and professional credibility;
- Customer, client, and stakeholder confidence;
- Recognition of employee achievements and organisational successes;
- Awareness of OHI Group's capabilities, values, and contributions.

Employees are encouraged to:

- Share official OHI Group and operating entity communications;
- Engage positively with company content;
- Highlight professional achievements and milestones;
- Participate in relevant industry discussions;
- Promote initiatives relating to innovation, sustainability, safety, quality, professional development, and organisational success.

Employees should ensure that any content shared publicly is accurate, respectful, and consistent with this Policy.

The Head of Corporate Communications can provide guidance, approved assets, and key messages where required.

6. DO's and Don'ts

All employees, workers, and third parties are expected to exercise sound judgement when using social media and digital communication platforms.

Do

Employees should:

- Use social media responsibly, professionally, and in accordance with OHI Group values.
- Share approved company news, achievements, thought leadership content, and publicly available information.
- Disclose their connection to OHI Group or the relevant operating entity when discussing company-related matters.

- Seek guidance from the Corporate Communications team when unsure whether content is appropriate for publication.
- Report inaccurate information, misinformation, negative commentary, or potential reputational concerns relating to OHI Group.
- Respect copyright, intellectual property, confidentiality, privacy, and data protection requirements.
- Follow customer, client, partner, supplier, and contractual communication requirements.
- Use approved logos, branding, imagery, and messaging when authorised.
- Ensure content shared online reflects positively on themselves and the organisation. Retaliation or adverse treatment of individuals who raise concerns in good faith; and
- Any other conduct that may adversely affect the rights, dignity, health, safety, or wellbeing of employees, workers, communities, or other stakeholders.

Don't

Employees must not:

- Present themselves as an official spokesperson for OHI Group or any operating entity unless specifically authorised.
- Create social media accounts, pages, groups, websites, blogs, or digital channels representing OHI Group or its brands without prior approval.
- Use OHI Group logos, trademarks, branding, or corporate assets on personal accounts without permission.
- Publish confidential, commercially sensitive, proprietary, personal, customer, client, or business information.
- Share content that could reasonably be considered defamatory, malicious, misleading, discriminatory, harassing, abusive, threatening, or harmful.
- Engage in online behaviour that could reasonably bring OHI Group, its businesses, employees, customers, clients, partners, suppliers, or stakeholders into disrepute.
- Participate in political, religious, or controversial discussions in a manner that may create reputational risk due to their association with OHI Group.
- Tag customers, clients, partners, suppliers, government representatives, or senior stakeholders without appropriate approval.
- Share internal communications, screenshots, meeting discussions, documents, emails, systems information, passwords, or cybersecurity-related information.
- Use AI-generated content that could mislead audiences or misrepresent OHI Group, its people, capabilities, services, products, projects, or achievements.
- Publish content that breaches applicable laws, regulations, contractual obligations, or professional standards.

7. Business, Client and Operational Content

All content relating to OHI Group businesses, customers, clients, projects, services, facilities, operations, employees, commercial activities, or third-party relationships must be treated with appropriate care.

Employees must not publish, share, distribute, upload, or otherwise make publicly available any:

- | | |
|--|-----------------------------------|
| • Photographs; | • Commercial information; |
| • Videos; | • Internal documents; |
| • Drone footage; | • Case studies; |
| • Workplace, operational, or facility imagery; | • Product or service information; |
| • Customer or client-related content; | • Employee-related content; or |
| • Project information; | • Other company-related material |

without appropriate prior approval.

Approval may be required from:

Head of Corporate Communications; and

The relevant business, customer, client, or authorised representative where applicable.

This applies to both official company accounts and personal social media accounts.

Employees must not:

- Take photographs, videos, recordings, or other digital content in controlled workplaces, customer locations, operational facilities, or business environments for personal social media use unless approval has been obtained.
- Publish content obtained through company systems, customer portals, collaboration platforms, internal communications, business applications, or operational systems.
- Share information that may compromise confidentiality, contractual obligations, security requirements, customer relationships, or business interests.

Certain locations, facilities, customers, industries, or operations may be subject to enhanced security, regulatory, contractual, or confidentiality requirements. Employees must comply with all applicable restrictions relating to photography, videography, recording, digital communications, and information sharing.

Employees must not use AI-generated images, videos, audio, or synthetic media in a manner that could misrepresent:

- OHI Group;
- Its operating entities;
- Employees;
- Customers;
- Clients;
- Projects;
- Services;
- Products; or
- Business capabilities.

8. Official and Personal Use

Employees may discuss OHI Group or its operating entities online provided it is clear they are not speaking on behalf of the organisation.

When commenting on company-related matters from personal accounts, employees should include a disclaimer such as:

"The views expressed are my own and do not necessarily represent those of OHI Group or its operating entities."

The use of a disclaimer does not remove an employee's responsibility to comply with this Policy or any other applicable company policies and procedures.

Only authorised individuals may issue official statements, announcements, or responses on behalf of OHI Group or its operating entities.

Senior leaders, executives, and managers should exercise additional caution because their personal views may be perceived as representing the organisation, even where a disclaimer is included.

Employees may identify OHI Group or an operating entity as their employer on professional networking platforms such as LinkedIn.

Information included on profiles should be:

- Accurate;
- Professional;
- Current; and
- Consistent with the individual's role and responsibilities.

9. Media Enquiries

Any enquiry from:

- Journalists;
- Media organisations;
- Bloggers;
- Podcasters;
- Influencers;
- Industry publications;
- Online media platforms; or
- Other external commentators

regarding OHI Group, its operating entities, customers, clients, employees, businesses, services, projects, or operations must be referred immediately to the Corporate Communications team.

Employees must not provide:

- Statements;
- Comments;
- Interviews;
- Photographs;
- Background information;
- Opinions; or
- Company-related information

without prior authorisation.

All media engagement must be coordinated through Corporate Communications to ensure accurate, consistent, and appropriate communication.

10. Confidentiality and Legal Compliance

Employees, workers, and third parties must protect confidential, commercially sensitive, proprietary, personal, customer, client, and business information at all times.

Such information must not be disclosed through social media, digital platforms, messaging applications, online forums, or any other public or unauthorised channel without appropriate approval.

Examples of confidential information include:

- Customer and client information;
- Commercial proposals;
- Tender submissions;
- Pricing information;
- Contract values;
- Financial performance;
- Business strategies;
- Unannounced projects or activities;
- Health, safety, security, environmental, or operational incidents;
- Employee information;
- Supplier and business partner information;
- Internal policies, procedures, systems, or communications;
- Information subject to contractual, regulatory, or confidentiality obligations.

Employees and third parties must comply with all applicable laws, regulations, contractual obligations, and OHI Group policies in the jurisdictions where the Group operates.

This includes, but is not limited to:

- Data protection and privacy legislation;
- Copyright, trademark, intellectual property, and licensing requirements;
- Competition and anti-trust legislation;
- Anti-bribery, anti-corruption, and anti-money laundering requirements;
- Confidentiality obligations relating to customers, clients, partners, suppliers, and employees;
- Export control, sanctions, and trade compliance requirements where applicable;
- Industry-specific regulatory obligations; and
- Customer or contract-specific communication requirements.

Employees must not use social media or digital communication platforms in any manner that could:

- Breach legal, regulatory, contractual, ethical, or professional obligations;
- Compromise confidential information;
- Damage business relationships; or

- Harm the reputation, interests, or commercial position of OHI Group, its operating entities, customers, clients, partners, suppliers, or employees.

11. Crisis and Issue Management

If you become aware of:

- Negative commentary;
- Misinformation;
- Reputational threats;
- Potential media issues;
- Fake accounts impersonating OHI Group or its businesses;
- Cybersecurity concerns;
- Sensitive online discussions; or
- Content that may adversely affect OHI Group or its stakeholders;

do not respond independently.

Immediately notify:

- Your line manager; and
- Head of Corporate Communications.

Timely reporting enables OHI Group to assess the situation and respond appropriately, consistently, and professionally.

Employees should not:

- Engage in arguments online;
- Attempt to correct misinformation independently;
- Delete or amend potentially sensitive content without guidance; or
- Escalate online discussions.

Once a concern has been identified, employees should preserve relevant information and seek advice from Corporate Communications.

12. Think Before You Post

Before publishing, sharing, commenting on, or engaging with any content online, employees should consider:

- Is it accurate?
- Is it respectful and professional?
- Is it appropriate to share publicly?
- Does it contain confidential, personal, customer, client, or commercially sensitive information?
- Could it negatively affect OHI Group, its operating entities, customers, clients, partners, suppliers, or colleagues?
- Would I be comfortable seeing this content publicly associated with myself and the organisation?
- Would I be comfortable if this appeared on the front page of a newspaper or was shared widely online?

If there is any uncertainty, employees should not publish the content and should seek advice from the Corporate Communications team.

13. Monitoring

OHI Group reserves the right to monitor publicly available references to the Group, its operating entities, brands, and activities where this is necessary for legitimate business purposes, including:

- Reputation management;
- Brand protection;
- Legal or regulatory obligations;
- Security requirements;
- Customer or stakeholder protection; or
- Crisis and issue management.

OHI Group does not routinely monitor employees' private social media accounts.

However, the Group reserves the right to review publicly available content where there is a legitimate concern relating to:

- Breaches of this Policy;
- Misuse of company information;
- Reputational harm;
- Legal or regulatory risk;
- Harassment, discrimination, or inappropriate conduct;
- Cybersecurity concerns; or
- Other matters affecting OHI Group or its stakeholders.

Any monitoring or investigation activity will be conducted in accordance with applicable laws, regulations, privacy requirements, and internal policies.

14. Artificial Intelligence (AI) and Digital Content

OHI Group recognises that artificial intelligence (AI) tools and emerging digital technologies can support creativity, productivity, communication, and innovation.

However, employees must exercise appropriate judgement when using AI tools to create content intended for publication, internal communication, or external distribution.

Any AI-generated content must be reviewed to ensure:

- Accuracy and factual correctness;
- Appropriate representation of OHI Group and its businesses;
- Compliance with copyright and intellectual property requirements;
- Protection of confidential information;
- Appropriate disclosure where required; and
- Alignment with brand standards and professional expectations.

Employees must not enter confidential, commercially sensitive, customer, client, employee, personal, financial, technical, or proprietary information into publicly available AI platforms unless specifically authorised.

Employees remain personally responsible for any content published, shared, or communicated on behalf of OHI Group, regardless of whether AI tools were used in its creation.

AI-generated images, videos, audio, documents, or other synthetic content must not be used in a manner that:

- Misrepresents OHI Group, its people, capabilities, products, services, or activities;
- Creates false impressions;
- Fabricates events, achievements, customers, projects, or relationships; or
- Could mislead internal or external audiences.

15. Internal Digital Platforms

The principles contained within this Policy also apply to internal communication and collaboration platforms, including:

- Microsoft Teams;
- SharePoint;
- Viva Engage;
- Internal forums;
- Collaboration workspaces;
- Digital communities; and
- Other internal communication tools.

Employees should maintain professional standards and demonstrate respect, integrity, and appropriate judgement when communicating through internal platforms.

Employees must:

- Protect confidential information;
- Respect colleagues and stakeholders;
- Avoid inappropriate, discriminatory, offensive, or harmful content;
- Follow applicable information security requirements; and
- Use internal platforms responsibly.

Private groups, closed forums, and internal communication channels are not exempt from professional responsibilities.

16. Alignment with OHI Group Values

This Policy supports OHI Group's commitment to professionalism, integrity, respect, collaboration, accountability, and responsible communication.

Digital communication is an extension of our organisational culture. Every employee and representative of OHI Group has a role in protecting our reputation, strengthening relationships, and demonstrating the values that guide our business.

Through responsible digital engagement, we help to:

- Build trust with customers, clients, partners, suppliers, employees, and communities;
- Showcase the expertise and achievements of our people;
- Support innovation, collaboration, and knowledge sharing;
- Promote OHI Group's capabilities and contributions; and
- Protect the long-term reputation and success of the Group.

Employees are encouraged to speak up when they identify risks, misinformation, inappropriate online activity, cybersecurity concerns, or behaviour that may affect OHI Group, its people, customers, or stakeholders.

17. Further Guidance and Training

If employees are unsure about any aspect of this Policy, proposed social media activity, digital content, or external communication, they should seek advice from the Corporate Communications team before publishing.

Employees may be required to complete social media awareness, digital communication, information security, or responsible technology training from time to time.

Additional guidance may be issued by Corporate Communications or relevant functions to support responsible digital engagement across OHI Group.