Catena
Inspection & Engineering Services Ltd
Lifting Solutions & Supplies

CHR030 Social Media and Phone Policy

AUGUST 2025 | ISSUE 1

Statement and Purpose of Policy

Catena recognises that social interactions on the internet and via mobile phones is an important and integral part of life and, if used correctly, can offer valuable business opportunities. However inappropriate use of social media can be a serious drain on productivity and can also pose significant business risks.

It is our policy that the use of social media at any time, whether or not you are using our equipment, must comply with the rules set out in this policy if it may affect our business in any way.

It is also recognised that people do want to be in touch with others outside of work, and we do not have a policy of no phone use at work. This is subject to reasonable use and we may choose to implement such a policy at any time if phone use is at an unacceptable level. This could be companywide or department / person specific.

The purpose of this policy is to ensure that all staff understand:

a) The extent to which personal use of social media is permitted during work hours;
b) The limitations on their use of social media, whether used during or outside hours of work;
c) The types of social media that could expose them and us to legal liability; and
d) What is considered acceptable mobile phone use during working hours.

This is a statement of policy only and does not form part of your contract of employment. We may amend this Policy at any time, in our absolute discretion

Who and What does this Policy apply to?

This policy and the rules contained in it apply to:

a. All our staff, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (**Staff**);
b. Use by staff of websites specifically aimed at social interactions such as Facebook, Instagram, LinkedIn, Wikipedia, TikTok, Threads and X (this list is not exhaustive) as well as blogging, participating in wikis and the use of interactive features or the ability to post or publish comments or information (including video, audio, photographs and text) with other people on other websites (**Social Media**);
c. Use of Social Media for business and/or personal purposes, whether or not during working hours and irrespective of whether our equipment or resources are used.
d. Use of mobile phones during working hours (working hours are any hours for which you are being paid, regardless of shift pattern)

This policy should be read in conjunction with CHR025 GDPR Policy and Procedure.

Who is responsible for this Policy?

The IMS Manager has general responsibility for the oversight and updating of this Policy. All Staff have personal responsibility to ensure compliance with this Policy. Managers have special responsibility for leading by example, ensuring that members of Staff are familiar with this Policy and for monitoring and enforcing compliance.

Business and Personal Use of Social Media

All media enquiries (including requests for comments for publication on Social Media) should be directed to the IMS Manager. If you are contracted by a media representative or asked for comment for publication about us or otherwise in connection with your employment, you should not respond unless you have been given written approval by the IMS Manager,

Only Staff specifically authorised by the IMS Manager (**Authorised Business User**) may use Social Media on our behalf as an organisation or post comments on any of our Social Media accounts or profiles. If you are authorised to do this, then we may require you to undergo training before undertaking such activities and you will be required to comply with additional guidance and/or instructions concerning these communications.

Guidance on Use of Social Media

Personal Capacity: Unless you are an Authorised Business User, when using Social Media:

a) You should make it clear that you are speaking in your personal capacity and not as our representative, communicate in a way consistent with that and if you choose to include contact information this should be your personal, not work contact details; and
b) If you do elect to disclose your connection to us, then you must clearly and expressly state that your views do not represent those of the employer. If you leave our employment it is expected that this es reflected in employment sections of any Social Media accounts.

Permanent form: It is always useful to bear in mind when posting any Social Media content or comment that they may be permanently and publicly available and that you may not be able later to delete or remove them. You should ensure that your communications are consistent with the image that you would like to present publicly including to us and any future employers, colleagues, friends, business contacts and the world at large.

Personal liability: Remember that you are personally responsible and may be legally liable for what you communicate on Social Media. Public statements of this type can create legal issues in a number of different ways including being defamatory, breach of confidentiality, infringement of intellectual property or amounting to unlawful harassment.

Taking care to avoid misunderstanding: Before posting comments, think about whether, even if innocently meant, they could be misconstrued in any way that creates legal problems or reputational damage for us or you. Steer away from commenting on sensitive topics relating to us or your employment. Such views might damage our reputation even if you make it clear the views expressed are personal.

Respecting privacy and confidentiality: All of us have information that we prefer to keep private. Do not post anything related to your colleagues or customers, clients, business partners, suppliers, vendors or other stakeholders without their written permission or in breach of this Policy.

Representing intellectual property: If you post or reference material that is protected by intellectual property rights, you should satisfy yourself that you have taken steps to avoid legal liability such as appropriately referencing sources and ensuring the citations are accurate, If you are an Authorised Business User and have questions about whether a particular post or upload to our Social Media accounts or profiles might violate anyone's copyright or trade mark then you should check with the copyright / trademark holder and/or the IMS Manager in advance.

Prohibited Uses of Social Media

Your communications through Social Media, like all other modes of communication, must not breach our disciplinary or workplace rules or any other policy and/or procedure and must not causes us to be in breach of obligations we owe to others.

For example, you must not use Social Media in any way that:

a) Breaches obligations of confidentiality which you owe to us or any third party or which causes us to breach duties of confidence which we owe to any third party;
b) Breaches the rights of any other staff member or third party to privacy, data protection and confidentiality or which amounts to bullying or harassment;
c) Is offensive, insulting, discriminatory or obscene;
d) Poses a threat to our trade secrets, confidential information and intellectual property;
e) Infringes the intellectual property rights of any other person or entity;
f) Defames, disparages or causes reputational damage to us or to any party with whom we have a business relationship, such as suppliers or customers;
g) Breaches or causes us to breach any law or the rules or guidelines of any regulatory authority relevant to our business;
h) Breaches data protection rules;
i) Breaches our rules, policies or procedures for the use of our IT systems or other equipment or resources;
j) Is dishonest, improper, unethical, misleading or deceptive (eg pretending to be someone);

k) Is likely to either directly or indirectly damage your reputation or our reputation.

You may not use our logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without prior written permission.

Information relating to business contacts that you make in the course of your employment amounts to confidential information and belong to us

You must not give references for any person on a social media site (including professional networking sites) on which our identity as your employer is shown in public or private part of the site. This applies whether the reference is positive or negative. The reason for this is that such references may otherwise be attributed to us and create legal liability both for us and for you personally as the author.

Monitoring

Information stored in our IT systems belongs to us. You should have no expectation of privacy in any communication, document, information file, post or conversation (**Information**) which you send or receive, access, print or store using our IT systems. In particular we may:

a. Intercept, monitor and read any Information or activities using our IT Systems, including Social Media use, to ensure compliance with our rules and for our legitimate business purposes. This may include use of recording devices or other surveillance methods, keystroke monitoring and other technologies; and
b. Retain copies of Information to store copies of such data or communications after they are created and delete such copies from time to time without notice.

Monitoring Social Media use will typically be conducted in accordance with an impact assessment that we carry out to ensure that monitoring is necessary and proportionate. Monitoring is in our legitimate interests and ensures that this Policy is being complied with. For the purposes of the law on data protection, the Employer is the data controller of the personal information in connection with your employment. This means that we determine the purposes for which, and the manner in which, your personal information is processed. The person responsible for data protection compliance is the IMS Manager.

Monitoring will normally be carried out by our IT Provider or another designated third party provider of this service.

Personal information obtained through monitoring may be shared internally, including with members of the HR team, your line manager, managers in the business area in which you work and IT staff, if access to the information is necessary for the performance of their roles. Information is only shared internally if we have reasonable grounds to believe that there has been a breach of this Policy. We will not share information gathered from monitoring with third parties, unless we have a duty to report matters to a regulatory authority or law enforcement agency.

You have a number of rights in relation to your personal information, including the right to make a subject access request and the right to have your information rectified or erased in

some circumstances. You can find out more about these rights and how to access them in CHR025 GDPR Policy and Procedure. If you believe we have not complied with your data protection rights, you can complain to the Information Commissioner.

Access to Social Media may be withdrawn in case of misuse.

What is acceptable use of a Mobile Phone during Working hours?

For the purposes of this policy, we class working hours as any time you are being paid for, regardless of contracted hours.

Unacceptable use of a mobile phone is when this impacts on your ability to work, affects quality or safety, or is disruptive to others in the workplace.

If you physically have to stop working and remove PPE or leave your workspace, then this could be generally taken as unacceptable.

Exceptions to this are in cases of genuine emergency contacts or where the company has pre-agreed you are able to do this due to an expected contact.

Some employees or departments will use their mobile phones for working purposes such as accessing emails, making calls or using the internet for research. Therefore it is not an automatic assumption that anyone using their phone is automatically using it for personal reasons.

If we have concerns over phone use, we will conduct a risk assessment to determine any actions to take.

Breaches of this Policy

We must all contribute to protecting the business reputation of Catena. If you see content in Social Media that is defamatory, false or disparages or reflects poorly on our organisation or our stakeholder, you should contact the IMS Manager.

Staff who breach this Policy:

a) Will be required to disclose relevant passwords and login information and to otherwise co-operate with our investigation;
b) May be required to remove the offending internet postings, comment or information;
c) May be asked to store their mobile phone in a locker or offsite; and
d) May be subject to disciplinary action up to and including dismissal.