# Capgemini

SOCIAL MEDIA
CODE OF CONDUCT

Social media both inside and outside the Group have transformed the way we interact. Online collaboration enables people to share knowledge and ideas regardless of rank, title, or experience. It's a way for us to take part in conversations around the work we do at Capgemini and show our expertise in these areas.

While this brings huge benefits, it also comes with certain risks and responsibilities. This policy sets out the parameters for activity in this area, empowering engagement in social media but establishing the accountabilities that come with it. It complements existing policies including the Code of Business Ethics, and our Cybersecurity Acceptable Use Policy.

This policy applies to all employees of the Capgemini Group and must be implemented by all Group companies.
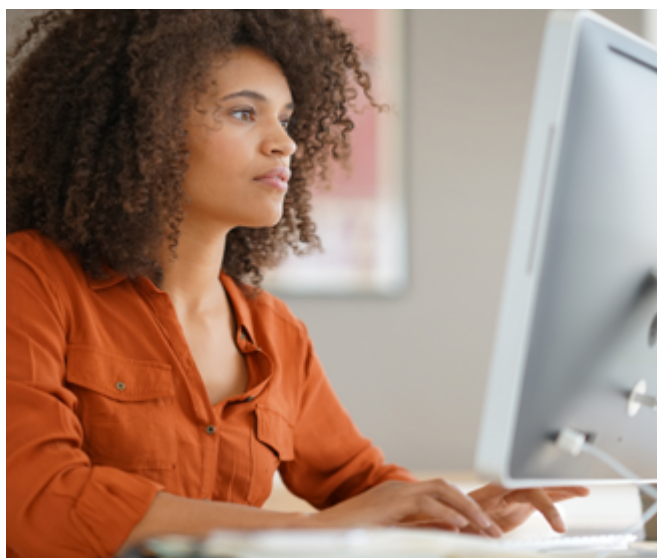
THREE GUIDING PRINCIPLES

We have established three principles that should guide all of us in every interaction online.

1 GET ENGAGED: ACT AS A ROLE MODEL

We encourage our employees to make the most of the opportunities offered by social media to demonstrate leadership, champion our capabilities, humanize our business and celebrate success.

2 GET THE BASICS RIGHT: SAFEGUARD YOUR ACCOUNT AND OUR NETWORK

We apply the same rules of personal behaviour online as we do offline. All employees must comply with the law, behave ethically, and prioritise information security. You must never forget that your online behaviour reflects both you and the business; your social posts are permanent.

3 PROTECT THE BUSINESS: THINK, BEFORE YOU POST

While we encourage employees to celebrate our successes and champion our capabilities, we must not give away commercially sensitive information: always protect clients', the Group's, and suppliers' confidential and other proprietary information.

REQUIREMENTS

The principles are underpinned by 10 requirements.

1. Don't share client information.
- Never share information around clients that is not in the public domain (e.g. already in a press release) including the names of clients or client employees, commercial information relating to a client's activities, or anything else that could be used to identify a client without express written permission.
- Only share information that is already in the public domain.
- Always protect clients', the Group's, and suppliers' confidential and proprietary information, and personal data*
- This is a contractual and legal requirement; breaches are subject to significant fines and the possibility of criminal prosecution.

Don't say	Do say
Very happy to announce that Capgemini has just been awarded a 6-month contract to overhaul Client X's' mobile payment processing platform, in partnership with Partner Y.	*Nothing! Do not say anything about the win, including the client or partner names, industry, or the topic. Do reshare official announcements made by Capgemini communications teams.*

2. Protect your colleagues.
- Do not share detailed information about team members' individual roles or contributions to specific projects.
- Do not share colleagues' personal data*, including their picture, without their permission.

Don't say	Do say
Congratulations to all the team on wrapping up a successful client delivery. In particular: Rachael Stevens: project lead; Sam Bryant: account executive; William Fournier: CRM expertise; Charlotte Yates: machine learning engineer	Really proud of my team for delivering such great work over the past 8 weeks and for making our client so happy! *And it's okay to tag colleagues – it's how social works – just don't go into detail about what each of them actually does.*

3. Know the rules.
- You are responsible for what you publish.
- Read, understand, and follow the company's Code of Business Ethics , Data Protection Policy, and the Group Cybersecurity requirements, outlined in the Acceptable Use Policy, as well as the Competition Laws Policy.

4. Be secure.
- Use a secure password, update it regularly, and never share your login information with anyone.
- Do not use your corporate email address to create personal social media accounts.
- Never publish images of your company computer screen, security pass, or other identifiable security features.

5. Observe copyright law.
- Pictures, videos, copy, and other content owned by others must not be used for our own commercial benefit.
- Do not post links to other websites, posts or pages without first checking that such sharing is authorized and that the content is lawful.

6. Be respectful.
- Never publish material that is obscene, racist, sexist, pornographic, sexually exploitative, or in any other way discriminatory, threatening or harassing, personally offensive, defamatory, or illegal.

7. Be transparent.
- Do disclose your association with Capgemini when discussing Capgemini matters.
- Always be honest about your role and position within the company; do not overstate your seniority and therefore authority.
- Only authorized company spokespeople may represent Capgemini's official positions online; be clear that you are expressing your own views and not those of the business.

Don't say	Do say
We believe the future of work is 100% remote.	I believe the future of work is 100% remote.

8. Don't criticize.
- Do not say anything disparaging about our business partners, competitors or colleagues.

9. Be constructive.
- Use social media to build relationships and share insights.
- By all means, engage in healthy debate – but always respect the views of others, especially on topics of race, religion, politics, and gender.

10. Think before you post.
- However informal, content published online is shareable and searchable forever; even private posts can be copied and shared, potentially ending up in international media.
- Always assume that any personal social media activity can be linked by someone to your professional profile and therefore your employer.
- If in doubt, ask your manager or local HR representative before you post.

If you have any questions or require further information, please contact your local communications team.

*Personal data is defined as any information that would allow the identification of an individual