



Digital Working Policy.

Introduction

We aim to create a culture where all team members are treated fairly and with respect to establish great working relationships and to ensure all team members are working within a safe and fulfilling working environment.

This policy sets out Cove Communities expectations on the use of digital resources, email and internet usage and social media. It reminds team members of the standards of behavior expected of them when they are using computers and electronic information as tools to support the company's business.

Scope

For the purposes of this policy, digital resources include computers, computer networks, email, telephones, voicemail, copy machines, mobile devices (including smartphones, mobile phones and tablets), access to the Internet, messaging and other electronic technologies.

For the purposes of this policy, social media is any online platform or app that allows parties to communicate instantly with each other or to share data in a public forum (this includes private/closed groups on social platforms).

This includes social forums such as Twitter, Instagram, Facebook, and LinkedIn. Social media also covers blogs, video and image-sharing websites such as YouTube.

Team members must use good judgement when transmitting, disseminating or posting information using digital resources. Team members should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. They should follow these guidelines in relation to any social media that they use.

You must not disclose or share your password with anyone, apart from the IT department on request, for purposes of support.

Team members may not speak on Cove's behalf, whether using digital resources, or otherwise communicating electronically or on the internet, without the proper authorisation from the Cove Communities UK Marketing Department.



Use of Technology at work

Technology resources are provided to Cove team members primarily for the purpose of conducting company business and enabling the person to whom it is assigned to perform their job-related duties. It is the responsibility of the team member to use these resources in a manner consistent with Cove policies as well as UK law. Personal usage should not occur during working time and should not disrupt the normal work duties of other team members during their working time. Working time does not include breaks, meal periods or time before and after work.

If it is in the remit of your role, to transmit customer data to others (either internally or externally), for the avoidance of doubt, customer information is any personal identifiable information such as phone number, email address, name, address, etc. Attachments containing personal information must be password protected, and you must not transmit the password to the recipient via email, use another medium such as SMS or Teams.

Use of email and internet at work

Email and internet access are provided to Cove team members primarily for conducting company business. It is the responsibility of the team member to use these tools in a manner consistent with Cove policies as well as UK law. Personal usage should not occur during working time and should not disrupt the normal work duties of other team members during their working time. Working time does not include breaks, meal periods of time before and after work. All messages distributed via Cove's email system or via the internet using Cove's technology resources are Cove property. It is the team member's responsibility to use email and the internet in such a way to secure, encrypt sensitive data, prevent the loss of data due to theft, compromise and/or viruses and malware.

Cove UK team email privacy

Cove UK's privacy settings for email require that each employee's email display includes specific information: first name, surname, park name, and the Cove UK identifier. For example, an email address might look like joe.blogg@cove.co.uk, with the display name formatted as *Joe Bloggs | Seal Bay*. This format ensures that both internal and external recipients see the full name and associated park, promoting clarity and professionalism in communication.

GDPR requires that personal data, such as names and work details, be processed lawfully, transparently, and only as necessary for the intended purpose. Since including an employee's name, park name, and company identifier (Cove UK) serves a legitimate business interest—namely, identifying the sender in professional communications—this use can fall under lawful processing grounds. Additionally, Cove UK should ensure that Cove team are informed about how their personal information will be used in email settings and provide a privacy notice explaining this.



Regular reviews of privacy settings and ensuring appropriate data minimization (e.g., not displaying more information than necessary) are also key practices for compliance.

Use of social media at work

Unless it is part of your job role, team members are not allowed to access social media from the organisation's computers or devices at any time.

We understand that team members may wish to use their own computers or devices to access social media while they are at work. Team members must limit their use of social media on their own equipment to their official rest breaks such as their lunch break.

Use of social media as part of your job

Cove UK encourages team members to make reasonable and appropriate use of social media if it is part of their work. It is an important part of how we communicate with our customers and communication with our team. You must only use approved social media platforms and check with the Marketing Department prior to use.

If part of your role is to manage social media activities, you must be always aware that, while contributing to our social media activities, you are representing Cove UK.

Team Members who use social media as part of their job must adhere to the following rules.

Team members should use the same safeguards as they would with any other form of communication about Cove UK in the public sphere. These safeguards include:

- making sure that the communication has a purpose and a benefit for Cove UK.
- obtaining permission from a manager before embarking on a public campaign using social media; and
- getting a colleague to check the content before it is published.

Facebook pages and groups for caravan sales are allowed with explicit permission from your manager but must meet the following criteria:

- Name of the group or page must not contain Cove or park name.
- Use of Cove branding is prohibited. Do not use Cove logos in your profile or cover photo.



- Admin access must be given to the marketing team at marketing@cove.co.uk

Please see caravan sales toolkit for more information.

Social media in your personal life

We recognise that many team members make use of social media in a personal capacity. While they are not acting on behalf of Cove UK, team members must be aware that they can cause damage, if they are recognised as being one of our team members.

Team members are allowed to say that they work for us. We recognise that it is natural for team to sometimes want to discuss their work on social media. However, the team member's online profile (for example, the name of a blog or a Twitter name) must not contain our company or group company name.

If team members do discuss their work on social media (for example, giving opinions on their specialism or the sector in which we operate), they must include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of my employer."

Monitoring use of technology resources

Use of technology resources may be monitored by Cove Communities UK, in its sole discretion, to determine that the usage complies with all policies, practices, and procedures. Information transmitted, received, created, modified, and/or stored on any technology resources is the sole property of Cove Communities. Users should have absolutely no expectation that any of their files, documents, electronic communications, and messages are private or protected from access by Cove Communities UK. Instead, Cove has the unconditional and unqualified right to access, monitor, review, copy, disclose, or otherwise use all electronic information, including, but not limited to computer files, emails, documents, messages and attachments transmitted, received, created, modified, and/or stored using the technology resources, whether generated for business or personal reasons. At any time and for any purpose it deems legitimate.

Cove Communities UK may access, monitor, review, disclose, remove or otherwise use any electronic information of its users, with or without notice. Monitoring is in Cove UK's legitimate interests and is to ensure that this policy on usage is being complied with. The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted. Information obtained through monitoring will not be disclosed to third parties (unless we are under a duty to report matters to a regulatory authority or to a law enforcement agency).



Cove UK Data Protection Officer (DPO) can be contacted at privacy@cove.co.uk

Access to particular social media may be withdrawn in any case of misuse and disciplinary action may result.

Email Etiquette

- Cove considers email as an important means of communication and recognises the importance of proper email content in conveying a professional image. Users should take the same care in drafting an email as they would for any other communication. Therefore, the company wishes users to adhere to the following email guidelines for all work-related emails:
- Cove's email style is informal. This means that sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards'. The use of Internet abbreviations and characters such as smileys, however, is not encouraged.
- Signatures must include your full name, job title, company name with address and contact information. It must be composed according to established Cove guidelines as outlined by the Cove Marketing Team.
- Users must spell check all emails prior to transmission.
- Do not use Reply All when responding to company-wide emails. Reply only to the appropriate group that will benefit from the response.
- Do not send unnecessary attachments, secure and encrypt sensitive data. Compress large attachments before sending them. Contact the Cove It Department for clarification on this procedure.
 - If you need to send files of over 30 MB, do not send these via email; contact the Cove IT Department to find alternate methods for sending the files (Such as through your Office 365 OneDrive account).
 - Do not write emails in capitals.
 - Only send emails of which the content could be displayed on a public noticeboard. If they cannot be displayed publicly in their current state, consider rephrasing the email or using other means of communication.
 - Only mark emails as important if they really are important.

Unacceptable Usage of technology resources



It is unauthorised and prohibited to use Cove technology resources for unethical or unlawful purpose and users must adhere to Cove's policies and procedures. Unauthorised or prohibited use of technology resources can result in disciplinary action, including and up to summary dismissal, and/or civil or criminal charges.

Activities prohibited by Cove include, but are not limited to:

- Use that violates any UK law.
 - Use that violates Cove's policies and procedures.
 - Use that impedes, interferes with, impairs, or otherwise causes harm to others' use of technology resources.
 - Use that compromises the security or confidentiality of any technology resources.
 - Transmission of any trade secrets or confidential information belonging to Cove, or its customers, vendors, or business partners without the proper authorisation from Cove Senior Management or above.
 - Use of technology resources in any way that may be threatening, discriminatory, harassing, defamatory, or otherwise illegal, including the disparaging or demeaning of others based on race, national origin, marital status, sex, sexual orientation or preference, age, disability, religion, citizenship, genetic information, veteran status, political beliefs, or any other characteristic protected by UK law.
 - Use of Cove technology resources to obtain and store sexually explicit material.
 - Engaging in any knowingly fraudulent activities or knowingly disseminating false or otherwise defamatory materials.
 - Unauthorised access of the computer, computer files or email accounts of other team members or sharing your account information or password with others without proper authorisation and coordination with the Cove IT Department.
-
- Any unauthorised or deliberate action that results in damage or disruption to Cove's computing systems, networks, or any other technology resources.
 - Use of technology resources to operate a business for personal financial gain.
 - Use that hides one's identity in work-related emails or misrepresents the sender as someone else.
 - Misusing, disclosing, or altering without proper authorisation, the confidential information of Cove, or its customers, vendors, or business partners.
 - Unauthorised installation, downloading, or use of software, programs, or files without the proper authorisation and coordination with the Cove IT Department.



- Transferring files from Cove’s computer systems to any other computer systems without express approval or coordination with the Cove IT Department.
- Use, transmission, duplication, or voluntary receipt of material for a commercial purpose that violates or infringes on any software license agreements, copyrights, trademarks, trade secrets, or patent rights of any person or organisation.
- Modification or removal of equipment without the appropriate permission and coordination with the Cove IT Department.
- Knowingly or negligently distributing computer viruses or other destructive programs into Cove’s systems or networks, or any actions that intentionally defeat virus scanning and detection software.
- Use that frivolously wastes or monopolises technology resources to the exclusions of others. For example, streaming media can use a great deal of network resources and should be used carefully to avoid interfering with the system’s efficient functioning.
- Allowing non-team members to access technology resources owned by Cove Communities UK.

Unacceptable usage of email & internet

In addition to those activities above, the following activities specifically related to the use of email and the Internet are prohibited by Cove, including, but not limited to:

- Sending or forwarding emails containing threatening, slanderous, defamatory, or illegal content, including the disparagement of others based on race, national origin, marital status, sex, sexual orientation or preference, age, disability, religion, citizenship, genetic information, veteran status, political beliefs, or any other characteristic protected by UK law. For example, the creation or communication of any sexually explicit or offensive messages, cartoons, jokes, ethnic slurs, or racial epithets are strictly prohibited. If you receive an email of this nature, you must promptly notify your manager.
- Sending credit card details, or other confidential information via email.
- Forwarding or copying a message or attachment with trade secrets or other confidential information without acquiring permission from the sender first.
- Unauthorised access or use of email accounts of other Cove Communities UK team members.



- Sending or forwarding junk mail or participating in pyramid schemes via e-mail or the Internet.
- Participating in forms of on-line gambling and gaming.
- Intentionally accessing Internet sites that include sexually explicit material or material that violates either Cove policies and procedures or UK law.
- Sending non-work-related solicitations or other personal emails either while on working time or that unduly disrupt the normal work duties of other team members while they are on working time.
- When sending out group emails be sure to use judgement as to whether your message needs to be sent to all parties in a particular group. All email accounts maintained on our email systems are property of Cove UK. Passwords should not be given to other people and should be changed according to the IT department policy. Email accounts not used for 60 days will be deactivated and possibly deleted.

Unacceptable usage of social media

Any communications that team members make through social media must not:

bring Cove UK into disrepute, for example by: criticising or arguing with customers, colleagues or rivals.

making defamatory comments about individuals, our business or other organisations or groups; or

posting images that are inappropriate or links to inappropriate content.

breach confidentiality, for example by: revealing trade secrets or information owned by Cove UK.

giving away confidential information about an individual (such as a colleague or customer contact) or organisation (such as a rival business); or

discussing Cove UK's internal workings (such as deals that it is doing with a customer or supplier or its future business plans that have not been communicated to the public).

breach copyright, for example by: using someone else's images or written content without permission.

failing to give acknowledgement where permission has been given to reproduce something; or

- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:



- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age.
- using social media to bully another individual (such as a team member); or
- posting images that are discriminatory or offensive or links to such content.

Disciplinary action

All team members are required to adhere to this policy. Breach of any portion of this policy may result in disciplinary action, up to and including summary dismissal and/or legal action.

You should inform the Cove IT Department of any violations of this policy, or any viruses or illegal messages received on the Cove UK technology resources, so the company may take appropriate action.

If you have any questions or comments about the Cove UK Digital Policy, please immediately contact the Cove IT Department, the HR Department, or your manager.