Capital Karts Information Technology (IT) Acceptable Use Policy

Introduction

You are required to read, understand and abide by the requirements of this policy.

Users have a responsibility to promote IT security and to follow the standards set out in this policy. Users must apply all technical and other means provided to them to safeguard the electronic information and systems within their care and use.

1. Purpose

The purpose of this policy is to establish the standard on privacy, confidentiality, and security in electronic communications at Capital Karts, to ensure that the IT systems and information are used for business purposes, and to prevent the misuse of Capital Karts IT resources, services, and activities.

This policy is intended to provide a framework for such use of the IT systems/ resources. Capital Karts IT systems means all technical hardware and software resources and tools that are used to create, store, use, share, archive, dispose/delete Capital Karts information or connect to Capital Karts IT application systems.

It should be interpreted that this policy has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to. Where new technology is required the User must follow the Data Protection Impact assessment procedure.

2. Scope

This policy applies to employees, agents, contractors, or other parties ('Users') who access Capital Karts' IT systems. Capital Karts seeks to promote and facilitate a positive and extensive use of Information Technology in the interests of supporting its employees and for providing services to our customers. This also requires appropriate and legal use of the IT systems made available.

3. Usage of Information Technology

IT systems provided by Capital Karts, containing Capital Karts information, or transmitting Capital Karts information must be used for the benefit of Capital Karts. Users are prohibited from using information technology in a manner that will harm or otherwise damage the reputation, integrity or financial position of Capital Karts or Capital Karts' IT environment.

Any Capital Karts information must be stored, handled and transmitted consistent with Capital Karts' General Data Protection Regulation (GDPR) policy.

4. Restriction on Use

IT system users must:

- Comply with all relevant GDPR regulation policies;
- Take reasonable steps to ensure the security of Capital Karts' information and equipment;

- Maintain individual accountability of each IT system user ID; this includes not permitting another user access to Capital Karts' IT systems using an assigned user ID; each user is accountable for any transaction performed under their user ID;
- Maintain the secrecy of all IT system passwords; this includes not sharing passwords with anyone including Capital Karts employees;
- Not install any software or additional hardware without approval from the IT department;
- Not disable or change anti-virus or other security software settings;
- Not change any predetermined security configuration;
- Not attempt to gain access to IT system facilities or Capital Karts information unless authorised to do so.

5. Personal Use

Reasonable personal use is permitted as long as it does not interfere with business use, is appropriate and is not excessive. Managers are responsible for interpreting what is appropriate and excessive. All personal use must still comply with the user's duty of care.

6. Privacy

All information, including e-mail messages and files, created, sent, retrieved or backed- up over Capital Karts IT systems are the property of Capital Karts, and should not be considered the private or confidential property of the user.

Capital Karts makes no representations to guarantee the privacy of information operated on Capital Karts IT systems except as required by law, regulation, written agreements or Capital Karts policy.

It is Capital Karts' policy to respect the privacy of its employees. However, for security, future infrastructure planning, specific site access restriction reasons and checking for compliance to policy, Capital Karts reserves the right to monitor all activities/communication to and from the Internet through or on its infrastructure.

Capital Karts may monitor, intercept, review, retrieve, filter, access, audit, store or block any electronic communications or other content on its IT systems, including stored voicemail and e-mail messages, with or without the specific knowledge of the users, as permitted by law, and may do so whether the messages are business-related or personal.

Users should be aware that the electronic communication records on their IT systems are discoverable in litigation (e.g., lawsuits, regulatory matters), internal or external research by Capital Karts, or audit purposes. This includes e-mail, voicemail, text messages, instant messaging conversations, documents, and any other retained communications. Such discovery can be done without the knowledge or consent of the Users.

7. Internet

Access to the Internet is provided to employees in connection with business purposes. Capital Karts reserves the right to revoke internet access or make any changes as deemed appropriate at any time without any notice, including the disallowing of sites and services. Capital Karts may limit access to Internet websites and services that are known or expected to contain malicious code, viruses or other threats to Capital Karts' IT environment.

- Access to the Internet from your work laptop or PC is only allowed while connected to Capital Karts network - either directly (e.g. while in the office) or remotely via our approved remote desktop solution.

- Any data or information that are confidential to Capital Karts, and its stakeholders, including but not limited to information on financial information, financial transactions, client information, business plans, business strategies, may not be transmitted through the internet without appropriate security.

- Access to any site representing, but not limited, to pornographic, sexual or racial themes or any offence punishable by law is prohibited.

- Participating in chat rooms or any forum not related to business use representing Capital Karts or otherwise is prohibited.

- Knowingly downloading any (i.e. getting/bringing) fi les, material, photos, music, software, screensavers, wallpaper not for authorised business use on any Capital Karts IT system is prohibited

- Publishing, distribution or display of any inappropriate, profane, defamatory, infringing, obscene, indecent, pornographic or unlawful material is absolutely prohibited.

- Unauthorised scanning, hacking, testing for security or other weaknesses of any Capital Karts or non-Capital Karts system, infrastructure, IT or non-IT related on the Internet and Capital Karts infonet is prohibited.

- Only authorised users are permitted to change the default settings of the Internet software configuration on IT hardware.

- No user is authorised to monitor or maintain their private or any other non-Capital Karts websites using Capital Karts network and/or equipment regardless of it being for a financial gain or not.

- Private use of any of Capital Karts equipment for conducting personal business for financial gain is prohibited.

8. E-mail and Messaging

Capital Karts maintains its e-mail system solely for conducting its business. Copies of messages created, sent, received or stored on the e-mail system are the property of Capital Karts. We cannot guarantee that electronic communications will be private. Users should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others.

Users must use the same care in drafting electronic communication as they would use for any other written communication and as reasonably expected in a professional communication. In particular, users must not use electronic messages to:

- Send chain letters, junk e-mail/messages, spam or any other duplicate electronic messages.
- Abuse, harass, stalk, threaten or otherwise violate the law or legal rights (such as rights of privacy and publicity) of others.
- Conduct business which is not related to Capital Karts business.
- Send material that is inappropriate, profane, defamatory, infringing, obscene, indecent
- or pornographic.
- Knowingly transmit or upload any material that contains viruses, Trojan horses or any other harmful programs or malware.

9. Social Networking

Users must use the same care in participating in Social Networking as they would use for any other written communication and as reasonably expected in a professional communication. All employees will be required to read the Social Media Guidelines to ensure they are aware of their responsibilities to Capital Karts when using social media.

10. Mobile Computing Devices

Mobile devices provided by Capital Karts and Capital Karts information on privately owned mobile devices must be used for the benefit of Capital Karts.

In addition to all other requirements, Users must:

- Take reasonable steps to prevent the physical theft of the mobile device or the information stored on it;
- Report lost or stolen IT systems immediately ;
- Be aware of surroundings and be mindful of the usage of IT systems in public places;
- Do not permit non-authorised individuals such as family members or others to use Capital Karts owned equipment.

10. Consequences of Breach

In the event of a breach of this policy by a User, Capital Karts may at its discretion:

- Restrict or terminate a User's right to use Capital Karts' IT systems;
- Withdraw or remove any material uploaded by that User in contravention of this Policy; or
- Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.