Alberni-Clayoquot Regional District

ELECTRONIC DEVICE, SYSTEMS AND COMMUNICATIONS POLICY

Policy Issued by: Board of Directors
Date Adopted: December 7, 2012

Purpose

The Alberni-Clayoquot Regional District (ACRD) recognizes electronic devices and communications are invaluable, as they can provide an effective, efficient and environmentally friendly tool to serve our constituents.

ACRD may provide its staff and Board members ("ACRD Representatives") with electronic devices, as well as access to and use of its electronic systems.

The purpose of this Policy is to ensure that ACRD's electronic devices and systems remain stable and secure and to ensure that ACRD's Representatives are aware of their rights and obligations regarding access to and use of ACRD's electronic devices and systems. Such electronic devices and systems may include, but are not limited to, computer systems and related hardware, software, and equipment or electronic devices of any kind (including blackberries, iphones, ipads, laptops, desktop computers, dictation equipment, printers, etc.).

Access to, and use of, ACRD's electronic devices and systems is a privilege, and accordingly, ACRD has the right to, at any time and with or without cause or notice, revoke, limit, or alter the ability to access or use ACRD's electronic devices and systems.

Scope

This Policy applies to the access and use of ACRD's electronic devices and systems, whether or not such access or use is made during business hours or personal time (e.g. weekends, before/after working hours, and scheduled breaks) and whether or not such access or use is made through computers or other electronic devices owned or operated by ACRD.

ACRD may amend this Policy in its sole discretion. If any amendments are made, we will notify ACRD Representatives.

Expectations

1. When accessing or using ACRD's electronic devices and systems, ACRD Representatives must at all times comply with all applicable ACRD policies and procedures. New and updated policies and procedures may be introduced as devices and systems evolve. We will provide you with notice of any changes.

2. ACRD's electronic devices and systems belong to ACRD. Keep this in mind at all times when using ACRD electronic devices and systems.

3. Use of ACRD electronic devices and systems is primarily for ACRD business.

4. ACRD recognizes that Representatives may use electronic devices and systems for incidental personal purposes. In engaging in personal use, ACRD Representatives must remember at all times that the devices and systems are in place for the purpose of public service and is paid for by the public. ACRD Representatives should conduct themselves accordingly.

5. ACRD Representatives must use good judgment and common sense in using electronic devices and systems. With respect to any use of ACRD electronic devices and systems, the following principles apply:

    - You have a duty to act in ACRD's best interests and not in a manner that:
        - conflicts with ACRD's mission, objectives, and reputation,
        - exposes ACRD to criminal or civil liability, or
        - compromises the integrity of the ACRD workplace.
    - Whenever you are communicating, including in social media, you may be considered a representative of the ACRD.
    - Whatever you do on ACRD electronic devices and systems, or related to ACRD business, may be accessible to the public and subject to the *Freedom of Information and Protection of Privacy Act*. Save for the statutory exceptions, ACRD Representatives should not send or collect anything he/she would not say in public nor be prepared to be publicly accessible.
    - You are obliged to protect confidential and personal information from unauthorized disclosure.
    - You must not conduct any illegal activity on or through ACRD electronic devices and systems. This includes but is not limited to theft, fraud and destruction of property, or comments that are defamatory, discriminatory, or harassing to others, including ACRD staff or other ACRD Representatives.
    - Be mindful that electronic activity can be tracked, monitored, and leave a lasting trail. Any e-mail or electronic file could be forwarded by the recipient.
    - You must not compromise the security, integrity or functionality of ACRD electronic devices and systems, or ACRD data or personal information held by ACRD.
    - Any personal activity should not interfere with ACRD business.

6. ACRD does not take responsibility for any personal documents, files, e-mails, or e-mail attachments on ACRD's electronic devices and systems. ACRD is not responsible for their safekeeping and reserves the right to remove them at any time and without prior notice to the ACRD Representative.

7. ACRD Representatives must not download or install any software on electronic devices and systems unless they have obtained the prior written approval of ACRD, with the exception of Apple application downloads on the ACRD iPADs.

8. All software is subject to licensing agreements. To prevent liability, ACRD Representatives must not remove, copy or install ACRD company software for use on a personal or non-ACRD computer. Conversely, ACRD Representatives should take care not to copy or install any software without authority.

9. ACRD will require devices to have security to protect them against unauthorized use, viruses and malware. All users of ACRD electronic devices and systems must adhere to any policies or procedures implemented by the IT Department. To help prevent viruses and loss of data, an ACRD Representative should only open attachments if the ACRD Representative knows what the attachments are, that they are coming from a reputable source, and the attachments have already been scanned for viruses or other destructive programs. ACRD Representatives should refrain from opening e-mail attachments that contain wav. files, video files or executable files as they may contain viruses.

10. Remote access via remote desktop and or VPN must be approved by the IT Department. All remote connections must be made behind a firewall-based router.

11. Remote access on personal computers or non-ACRD owned computers must have a current anti-virus program with current updates and must be behind a HW-based firewall router.

12. Electronic communications, including e-mail and text, are forms of business communication and ACRD Representatives should treat it as such. ACRD Representatives should be respectful, honest, and professional in all electronic communications. ACRD Representatives are expected to exercise the same care in electronic communication as they would for any other formal communication.

13. All e-mail sent outside ACRD by an ACRD Representative that relates to ACRD business should include the following information in the following format:

    Employee's Name
    ALBERNI CLAYOQUOT REGIONAL DISTRICT
    [Position]
    Tel:
    Fax:

This e-mail is confidential and may be privileged. Any use of this e-mail by an unintended recipient is prohibited. If you receive this e-mail in error please notify me immediately and delete it.

14. ACRD Representatives must not use ACRD's electronic devices and systems to access or use online gambling websites or pornographic websites, or to spam or impersonate others including the ACRD, or other ACRD Representatives.

15. ACRD Representatives must not use ACRD's electronic devices and systems for personal commercial, political, or fundraising activities without ACRD's advance written consent.

Security

16. E-mail communications are not necessarily a secure method of communication. If distributing confidential information, ACRD Representatives should consider sending it another way or make sure it is properly encrypted.

17. Protecting the confidentiality and security of ACRD's data, including personal information, must be a top priority. This applies to both paper files and electronic documents. ACRD Representatives play a crucial role in the protection of ACRD's information and must adhere to the following guidelines:

    (a) ACRD Representatives must take all necessary precautions to prevent unauthorized access to, and use of, ACRD's information, electronic devices and systems.

    Absent ACRD's advance written consent, ACRD Representatives must not disclose to others, including other ACRD Representatives and third parties, the passwords, log-in information, or other security measures used to access, use, or protect ACRD's electronic devices and systems.

    ACRD Representatives should refrain from using insecure public internet access (e.g. Internet cafes or coffee houses) for ACRD business due to security concerns.

    (b) ACRD Representatives must use their own password, log-in information, or other approved security measures to access or use ACRD's electronic devices and systems. Absent ACRD's advance written consent, ACRD Representatives must not seek, obtain, or use anyone else's account password or log-in information when accessing or using ACRD's Computer and E-mail Systems;

    (c) ACRD Representatives must keep their passwords strictly confidential. ACRD Representatives should never write down their passwords or leave them somewhere where someone else can see them. ACRD Representatives must

not save a Word document containing passwords, as this file can be easily accessed by others.

(d) If a ACRD Representative has reason to believe that security has been compromised, including if his/her password has been compromised or discovered by another person, the ACRD Representative must immediately inform the IT department and change their password immediately. ACRD Representatives must change their passwords every 90 days.

Mobile Device Specific Security Settings

18. Access to any mobile device configured for access to any ACRD systems, including but not limited to an ACRD email account, must be configured to lock automatically within a maximum of 10 minutes of inactivity and require a minimum of 4 digit password to unlock.

If an ACRD Representative suspects any access or use of ACRD's electronic devices and systems in breach of this Policy, the ACRD Representative should immediately contact the Manager of Administrative Services at the ACRD.

Consequences of Breaching this Policy

19. ACRD Representatives accept full responsibility for their own use of ACRD's electronic devices and systems.

20. ACRD Representatives in breach of any term of this Policy may be subject to a variety of actions depending upon the circumstances, including revocation of or limitations on access or use privileges of ACRD electronic devices and systems. Board members may be subject to censure. Employees may be subject to disciplinary action up to and including termination of employment. ACRD Representatives may also be held civilly or criminally liable depending upon the circumstances.

21. If you are uncertain whether you are compliant with this Policy, please immediately discuss your concerns with the Manager of Administrative Services at the ACRD.

Monitoring of Access and Use

22. ACRD may monitor, record and review the access and use of its electronic devices and systems from time to time as reasonably required by ACRD. Such monitoring, recording or reviewing may be done for various purposes, including but not limited to: ensuring system integrity, evaluating equipment and software use, fulfilling ACRD's duties and obligations, protecting ACRD's proprietary and confidential information, determining compliance with this policy, and investigating a potential breach of ACRD policies or the law. ACRD may also require access and a record of use and information on a device or system to comply with legal and regulatory requirements, including Freedom of information and protection of privacy legislation.

23. ACRD will generally only monitor and record access and use when there is, in ACRD's view, good cause or a legal obligation to do so. ACRD will ensure that any monitoring or recording of information is limited to what is reasonably required in the circumstances. ACRD Representatives should not expect their use of ACRD electronic devices and systems are private from ACRD.

Questions

Any questions regarding the terms of this Policy should be directed to the Manager of Administrative Services at the ACRD.

Acknowledgement & Agreement

I acknowledge that I have read and understand this electronic device, systems and communications policy, that I will comply with the terms of this policy, and that I will ensure that any employees or volunteers working under my direction comply with the terms of this Policy. I understand the potential consequences of violating the policy as set out above.

All electronic devices issued to be by ACRD belong to the ACRD and I will return them to the ACRD, without alteration, immediately upon request. In some circumstances, you may be able to arrange to purchase a device or software license from ACRD.

Name: _____

Signature: _____

Date: _____

Witness: _____