AC30 AUTHORIZED USE AND SECURITY OF COMMUNICATION EQUIPMENT AC30

Effective Date: 01 February 1997
Revised Date: 15 November 2017
Last Reviewed Date: 15 November 2017

POLICY

1. The Delta Police Department ("Department") will ensure compliance in the use of all automated systems consistent with the rules approved by the Triumvirate / Information Technology Sub-Committee at CPIC Services.

2. The Department will ensure all employees operate communication equipment, communication devices and software in accordance with Statutory Law, Provincial Policing Standards and Department Policy.

3. This policy applies to all users of Department communication equipment and software as authorized by the Chief Constable.

REASON FOR POLICY

4. To identify responsibilities and requirements of the users and to provide guidance as to the use of Department and personal communication equipment including desktop personal computers, laptops, wireless devices and related components, technologies, and supporting software.

RELATED POLICIES

AE16 – Security and Confidentiality of Records and Information
OC40 – Social Media

PROCEDURES

Ownership

5. All electronic communication equipment and software, and information and data installed or created on Department electronic equipment is the property of the Department. This includes all programs, documents, spreadsheets, databases, and methods or techniques developed using Department equipment and/or software.

6. All electronic documents related to the Department, including emails that are electronically created, received and retained by employees, or that are printed on paper and placed in a paper file are considered under legislation to be "Records" of the Department and as such are subject to all of the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act* (the 'FOIPP Act') and all record systems policies, such as those governing disclosure of CPIC or PRIME records.

Disclosure and Removal

7. Other than for approved Department business, and as authorized in legislation or related Department Policy, information or data on electronic equipment may not be:

   a) printed and disclosed;

   b) electronically copied to removable media, including diskettes, CDs, memory sticks or any other type or form of storage device; or

   c) downloaded or exported electronically to another individual or agency, whether public or private.

8. If in any doubt about the appropriateness of a request for information from a source outside the Department, employees must refer the matter to their supervisor, Information Technology Branch and/or the FOI Coordinator, or refer to related Policy **AE16 – Security and Confidentiality of Records and Information**.

Authorized Use

9. Employee use of Department communication equipment and systems, including, but not limited to hardware, software, wireless phones, data, programs, databases, internet resources or email resources (hereafter "electronic systems") is intended solely for activities which are necessarily incidental to the employment of the user. Department electronic systems are not intended for personal use, except as allowed by Section 18 and employees shall not have any expectation of privacy when using any Department electronic system. All electronic communications are considered to be Department records and shall be treated by employees in accordance with the FOIPP Act and any restrictions placed upon their use by the Department or by the sender of the communication

10. Equipment, systems and software owned and licensed to the Department may not be used for any activity in which an employee receives remuneration or "in-kind" service(s), other than those received directly from the Department.

11. Authorized use and access is defined as the level of access to a specific system granted by Information Technology Branch Manager or the PRIME Coordinator, and is subject to clearance and training. If in doubt about authorization, employees are to consult with their supervisor.

12. Department electronic systems and the data or records stored therein, may only be accessed and used for an authorized purpose, and shall not be accessed or used for personal reasons, or to benefit the employee or another person outside of the scope of the employee's employment.

13. Department issued computer and network equipment may not be used for:

    a) software piracy, forgery, or copyright violation;

    b) activities which violate another organization's privacy including hacking and cracking, unless required for police related activity;

    c) activities intended to disable, overload or circumvent the Department owned or other systems designed to protect the privacy of other users; and

    d) any activity which could adversely affect the work or reputation of the Department.

14. Only software and hardware that has been approved and purchased by the Department is to be used on or attached to the Department's computer equipment.

15. Software installed on Department computers shall only be used in accordance with the license and copyright agreements for the specific software in use. Generally, one license is required for each installation, unless the software specifically states concurrent use is allowed.

16. Computer software and hardware, including modems, printers, games, shareware, freeware, screen savers, or any other product or applications shall not be used or installed on the Department's computer equipment, regardless of their source, unless approved by Information Technology Branch.

17. Only Information Technology Branch employees may authorize the installation of computer software and hardware, to ensure that such items do not represent a security risk to the Department's network.

18. Incidental and occasional personal use of Department electronic systems is allowed, providing such limited use will not result in any measurable expense to the Department in time or materials and does not contravene any other provision of this or other Department policies and procedures.

Security

19. Information Technology Branch shall assign a User Identification ("UserId") to each user. Each user shall create a confidential password that will not be shared, except for pre-arranged group UserIds.

20. Users are accountable for all activities that occur under their UserId. Users are responsible for immediately reporting any known or suspected compromise of their UserId or password. If an irregularity is suspected, the Information Technology Branch will examine logs to determine if unauthorized usage has occurred. Passwords shall not be left unsecured or left where someone else can find them.

21. All users are responsible for changing their own passwords at least once every ninety (90) days. Passwords should be easy for the user to remember, but difficult for others to determine. Password parameters will be set by the Information Technology Branch.

22. The Information Technology Branch Manager shall provide for the performance of random audits of computer-related activities including all computer network traffic, including email, Internet, and MDT activity on all storage mediums. Audits may also be performed on the request of a Management representative.

23. Inappropriate, irregular or suspicious activities shall be reported to the Inspector, Human Resources Branch for appropriate action. Monitoring and reporting of abuses of this procedure shall not distinguish between business and personal use.

24. The disclosure to a third party of any electronic communication, received by a Department employee, that has been identified by the sender as confidential is strictly prohibited, except as authorized by the sender of the communication or the Department or as otherwise required by law.

25. For the purposes of this policy, the Information Technology Manager or delegate may access, monitor, review, copy or disclose any electronic communications made in any way at any time by employees. The Information Technology Manager may also access or monitor user activities within the electronic systems, including archived material of present and former employees, without the user's consent.

26. Employees shall report procedure violations to their appropriate supervisor, who in turn will submit a brief report concerning the alleged violation to the Inspector, Human Resources Branch.

Backup and Storage

27. The Information Technology Branch is responsible for the backup and off-site storage of all data and software stored in central-site facilities, including PC documents that are stored on network disk drives accessed by PCs. In instances where information cannot be stored centrally, (e.g. documents stored on the local C: drive) supervisors are responsible for ensuring that backups are being done frequently to adequately protect information not stored on centralized computers. This shall include arranging and coordinating off-site storage of data files as required.

Use of Personal Devices

28. For reasons of accountability, prosecution disclosure, safety, and compliance with legislation, employee work related electronic recordings

and communications shall be restricted to use of the communications systems provided by the Department.

29. Except in exigent circumstances, an employee shall not use a personal communication or recording device, text from and/or to their private personal numbers, or email between personal account addresses, in relation to Departmental operational, investigative or business matters. Exigent circumstances may include instances where there is strong possibility of losing the opportunity to record evidence and access to Department supplied equipment is not available.

30. If a personal device is to be or has been used for recording or communication in relation to an operational, investigative or business matter, the employee intending to or having done so must, as soon as practicable:

    a) advise their supervisor;

    b) transfer a complete copy of the recorded or communicated data to the relevant Department operational, investigative or business file on Department equipment; and

    c) after the recorded or communicated data has been transferred, delete the same on the personal device.

31. Personal electronic devices must not be connected to Department network or equipment systems, other than as required to transfer recorded or communicated data to Department equipment.

32. Personal devices may be connected to DPD Guest Wi-Fi network.

33. Emails, phone calls and other information, specific to Departmental operational, investigative or business matters, shall not be forwarded to personal accounts or phone numbers.

Internet and Email Use

34. Use of the internet and email by employees is restricted to Departmental business only, except as allowed by Section 18 of this policy. Internet access is provided to employees for research or system support purposes relevant to Departmental business. Supervisors, at their discretion, may

choose to block public internet access for specific employees and/or computer stations.

35. The downloading of non-executable files from the internet or other sources for business use is permitted. Examples of permitted files would include reports, Adobe PDF files, spreadsheets, and information flyers. Confirmation of the reliability of the source is required as viruses can be introduced to the Department network through spreadsheets and other documents.

36. The downloading of executable software (programs) is not permitted without written authorization from the Information Technology Branch Manager. Such software, if approved, must be checked for viruses before being executed.

37. Each supervisor is responsible for monitoring the use of the internet by employees under their authority. Minor violations of the policy may be dealt with by the supervisor. Violations of a serious nature shall be reported to the Inspector, Human Resources Branch for further action, if required.

Specific Internet Restrictions

38. The primary purpose of granting access to the internet, through Department electronic equipment, is to provide an information resource to Department employees for Departmental business. Except as performed in the furtherance of assigned duties, employees are not to:

    a) send or willingly receive any material that is obscene, or defamatory, or which has the potential to annoy, harass, or intimidate another person or group of persons;

    b) visit internet sites that contain obscene, pornographic, hateful or otherwise objectionable content;

    c) use the internet for illegal purposes;

    d) use continuous access technology such as "Push or Pull" common to many news services, or other Web sites that do not require user intervention to refresh information. Examples include PointCast, Audio, and Music;

e) use the internet in a manner that violates Statute law, B.C. Provincial Policing Standards or Department Policy; and

f) use the internet for social media (e.g. Facebook, Instagram, Twitter), streaming video (e.g. YouTube or Netflix), internet games and subscriptions to internet services unless authorized in the line of duty.

Specific Email Restrictions

39. Email is restricted to the conduct of Departmental business which directly relates to the employee's function at the Department, except as allowed by section 18 of this policy.

40. Email records are subject to disclosure access requests in accordance with the FOIPP Act. Employees are to be mindful that inappropriate language or comments could prove embarrassing to the person who created the email, as well as to the Department, if required to be released.

41. Any email, and the information contained therein, sent to an external service provider, is no longer under Department control and cannot be retracted or deleted by the sender. Employees sending emails shall use caution, and assess the sensitivity of the information they are sending and the external service provider's respect for the confidentiality of their email.

42. Email correspondence for external consumption is like any other correspondence and as such, professional business practices shall be adhered to in respect of the creation and content of email records. The following guidelines shall be adhered to:

a) use only professional language;

b) do not express personal opinions about individuals or situations, unless it is a specific task or requirement as part of your position or job function;

c) if there is a need to include confidential information, mark the text as "confidential". Text containing or commenting upon legal opinion or strategy shall be marked "confidential". With some exceptions, the Act provides for the protection of solicitor-client privilege and for the sheltering of advice given by "officers" of the Department;

d) in general, do not include any text or information that would not be suitable or could not be "made public". Use the same approach used when writing a letter to a citizen, or preparing a report for the Department;

e) do not send or willingly receive any material that is obscene, or defamatory, or which has the potential to annoy, harass, or intimidate another person or group of persons; and

f) do not use email in a manner that violates Statute law, B.C. Provincial Policing Standards or Department Policy.

43. Users may delete email or Police Records Information Management Environment ("PRIME") email once its usefulness has expired.

Management of Users

44. Information Technology Branch shall be notified of all changes to UserIds. This includes disabling the user's access temporarily or permanently, deleting the UserId, adding new users, changing access rights and advising of employee's location changes.

45. The Information Technology Branch Manager may provide written authorization to employees to have computer access outside their own work area and for off-site access to computers as these services become available.

46. Upon termination or transfer of an employee, all documentation, email programs, and all information remain the property of the Department.

47. Users shall surrender any hardware, software, and related Department documentation in their possession upon termination of their employment.

Firewall Security

48. In order to protect the security of the Department and CPIC, the following procedure on Firewall Security shall be adhered to:

a) only Information Technology Branch employees shall administer the Firewall; and

b) the Firewall shall stay on its own dedicated appliance. No other software, except Firewall or security related software shall be implemented on the Firewall appliance.

Policy Violation

49. When an Information Technology Branch employee encounters any suspected procedure violations by a user, the Information Technology Branch employee shall immediately:

a) de-activate the User's account; and

b) notify the Information Technology Branch Manager who will report to the Deputy Chief Constable for further action.

50. Only upon written approval from the Deputy Chief Constable shall the User's account be re-activated.

51. Employees violating this policy may be subject to discipline up to and including dismissal.