# FRANCES BAARD DISTRICT

# MUNICIPALITY

## INFORMATION COMMUNICATION AND TECHNOLOGY

## ACCEPTABLE USE POLICY

Version: September 2016

# Acceptable Use Policy for ICT Systems

## Table of Contents

## 1. BACKGROUND

The main of this policy is to enable employees to work productively while also ensuring the security of the Information Communication and technology (ICT) infrastructure, hardware, software, network and, crucially, the data on ICT environment. Given that technology is continually changing, employees play a significant role in ICT security. This policy provides a framework for users to follow when accessing ICT systems and the data on the ICT environment.

## 2. PURPOSE

This Acceptable Use Policy (AUP) for ICT Systems is designed to protect Frances Baard District Municipality (FBDM), employees, external stakeholders and other partners from harm caused by the misuse of ICT systems and data. Misuse includes both deliberate and inadvertent actions. The purpose of this document is to outline acceptable and prohibited use of FBDM ICT.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Everyone who is authorised to use/access ICT systems at FBDM is responsible for the security of ICT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how ICT impacts their role they should speak to their line manager or ICT manager.

## 3. DEFINITIONS

“Users” are everyone who have access to any of FBDM’s ICT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, customers and business partners.

“Systems” means all ICT equipment that connects to the FBDM network or access FBDM applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar Items commonly understood to be covered by this term.

“Social media” means and includes Internet technologies that facilitate and promote interactive communication, participation, and collaboration. Examples of social media include, but are not limited to, the web sites and applications Facebook, LinkedIn, Twitter, Tumblr, and YouTube.

# 4. SCOPE

This is a universal policy that applies to all users and all systems. For some users and/or some systems a more specific policy exists: in such cases the more specific policy has precedence in areas where they conflict, but otherwise both policies apply on all other points.

This policy covers only internal use of FBDM systems, and does not cover use of our products or services by customers or other third parties.

Some aspects of this policy affect areas governed by local legislation in local government (e.g., Municipal System Amendment Act 2003 and Municipal Finance Management 56 of Act 2003): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.

Staff members at FBDM who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

## 4.1 **Furthermore, the policy defines principles for appropriate utilisation of ICT facilities within the municipality. These include:**

- User access management;
- Password usage;
- 3G card usage;
- Network drive (P & O drives);
- Network and internet usage; and
- E-mail usage.

# 5. POLICY STATEMENTS

Any individual using the FBDM ICT facilities is deemed to have accepted this policy and is bound by it.

ICT facilities are provided to users primarily for municipality business purposes to support the municipality in achieving its mandate and strategic goals. This policy applies to all employees of the municipality, including contractors and consultants, who use ICT services and assets. This policy applies to all equipment that is owned or leased by the municipality

# 6. USE OF ICT SYSTEMS

All data stored on FBDM systems is the property of the municipality. Users should be aware that the municipality cannot guarantee the confidentiality of information stored on any system of the municipality except where required to do so by local laws.

The municipality systems exist to support and enable the business. A small amount of personal use is, in some cases, allowed. However the usage must not be in any way detrimental to users own or their colleagues productivity and nor should result in any direct costs being borne by the municipality.

The municipality trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the municipality's ICT systems. If employees are uncertain they should consult their line manager or ICT unit.

Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorised access is prevented. However, this must be done in a way that does not prevent or risk preventing legitimate access by all properly authorized parties.

The municipality can monitor the use of ICT systems and the data on ICT systems at any time. This may include (except where precluded by local privacy laws), examination of the content stored within the email and data files of any user, and examination of the access history of any users.

The municipality reserves the right to regularly audit networks and systems to ensure compliance with this policy.

## 7. DATA SECURITY

If data on the municipality's systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access ICT systems. Users must take all necessary steps to prevent unauthorized access to confidential information.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-municipality system any information that is designated as confidential, or that they should reasonably regard as being confidential to the municipality, except where explicitly authorized to do so in the performance of their regular duties.

Users must keep all their passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with the municipality's password policy.

Users who are supplied with computer equipment by the municipality are responsible for the safety and care of that equipment, and the security of software and data stored on those system, and on any other systems of the municipality that they can access remotely using ICT.

Because information on portable devices, such as laptops, tablets and smartphones, are especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure ICT systems.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the computer should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors, etc.) being imported into the municipality's systems by whatever means and must report any actual or suspected malware infection immediately.

## 8. USER ACCESS MANAGEMENT

The following steps will be followed for user access management for FBDM ICT systems.

| Situation | Acceptable outcome |
|---|---|
| Allocation of access rights to new employees or ICT system access request | • There shall be a formal user registration procedure for granting access to requested information systems and networks, either by logging a ICT service call or formal memo;<br>• Access rights to external consultants or contractors must be authorised by the by the Manager: ICT;<br>• Access rights to privileged systems must be formally screened and authorised by the Manager: ICT;<br>• Logon names shall be unique to each user and standardised;<br>• ICT Division shall review all user access rights periodically, and renewed or revoked when appropriate. The results of this review must be communicated to the affected users where feasible; and<br>• ICT Division shall also review all user accounts with administrative rights on the active directory to ensure only authorised users have admin rights; |

| | |
|---|---|
| Movement, Retirement, Suspension, and Termination of Employees | • Human Resource unit will notify IT in writing regarding of movement, retirement, suspension, and termination of employees<br>o Dismissal – access rights will be disabled immediately;<br>o Suspension – access rights will be disabled immediately until reinstatement;<br>o Resignation – access rights will be disabled on last day of work;<br>o Transfer to other municipalities – access rights will be disabled on last day of work; and<br>o Disabled accounts will be permanently deleted after 12 months. |
| Access to ex-users account | Line manager can request an extension for user account to remain active of a retiring, resigning or terminated employee, on conditions that:<br>• S/He submits a written memo to ICT manager requesting such extension;<br>• Extension is no longer than 30 days; and<br>• Identifies who will take responsibility of the account, for accountability. |

## 9. PASSWORD USAGE

Access to the FBDM ICT systems is controlled by the use of username and passwords. All Username and passwords are to be uniquely assigned to authorised users and consequently, individuals are accountable for all actions done on FBDM ICT systems done with their usernames. Users are not allowed to share their password with anyone else, including ICT personnel. All user account should be named accounts, relating directly to specific person. General Usernames like “students” or “cleaners” will not be accepted, unless a responsible person is identified in writing.

Users should also adhere to the following principles:

- Never leave the computer logged in with their account unlocked and unattended, they should always lock their computer before leaving;
- Using someone else login credentials;
- Writing down their passwords; and
- Attempt to access FBDM information that they are not authorized to access or view.

The following password management will be applicable:

- Passwords must be changed every 30 days;

- The systems shall allow only 4 attempts for incorrect logons where after the user account shall be locked;
- The user will be responsible for ensuring that the password remains secure. The user will be held accountable should the password be compromised due to negligent actions such as, writing a password down and leaving it accessible to others; and
- Employees who have any reason to believe or suspect that someone else is using their password must immediately notify ICT unit.

All users will have to comply with the requirement of the password policy attached to AUP.

## 10. 3G CARD USAGE

FBDM allocates 3G cards to users to allow them to be able to execute their duties remotely from FBDM premises.

All users are expected to use 3G cards only for work related tasks, and shall be responsible for ensuring usage do not exceed that maximum allocated amount. The user will be liable for any amount that exceeds the allowed limit. Users are not allowed to access any illegal materials nor use the 3G card for any illegal activities.

The usage of 3G cards should be strictly used for official tasks only.

Users may not borrow or allocate 3G cards to other users, without written permission from ICT unit. Users should notify ICT unit within 24 hours of any lost 3G cards.

## 11. NETWORK DRIVE

The municipality has implemented a file management server to be used by all authorised FBDM employees and other stakeholders. This is to ensure FBDM information on user's machine is accessible by all stakeholders who share the same interest on that information and to allow the information to be backed up and retrievable in the event of a user's machine getting lost or damaged.

Each network user is allocated his/her own network drive directory, were they can store their work related information and to keep their email archive files.

The network drive should be strictly used to store only work related items, ICT unit has the right to continuously verify all data stored on the network drive is work related, and if needs be, deleted any information which is:

- Not work related;
- Pirated;
- Illegal; and
- Have no value to FBDM.

The users are expected to utilise the server disk space in a responsible and acceptable manner, to ensure FBDM system do not run out of space.

## 12. NETWORK AND INTERNET USAGE

Network usage should be in line with the duties of the users, and care should be taken to protect the network from external threats, all users should comply with the following:

- ICT will ensure that users are only provided with direct access to the networked resources that users have been specifically authorised to use. Users are not allowed to modify network hardware or devices. Only administrators are allowed to configure network devices;
- Users are not allowed to install software that provides or manipulates network. Under no circumstances should users install any software on the systems unless otherwise authorised by ICT;
- ICT shall provide firewalls for secured access between the FBDM network and worldwide network. Attempts to by-pass the firewall are strictly prohibited;
- No personal hardware or devices are allowed on the network unless authorised by ICT;
- Avoid all illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations;
- Avoid all activities which are for personal benefit only that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, social media, playing networked video games and sending of chain email on the FBDM's ICT system);
- Avoid all activities that are inappropriate for FBDM to be associated with and/or are detrimental to the municipality's reputation. This includes pornography, gambling, inciting hate, bullying and harassment; and
- Circumventing the ICT security systems and protocols which FBDM has put in place.

## 13. EMAIL USAGE

Every user is accountable for his/her email account, the municipal email account should be used with care and not bring the municipal in disrepute. The following rules apply to the usage of the official FBDM email account:

- Not to disguise or attempt to disguise own identity when sending an email, and shall not forge or attempt to forge any email message;
- Not intentionally send any malicious material, such as a virus infected file, either internally or externally which might compromise the ICT systems and/or operations of the municipality; and
- All information transmitted via the municipality's Internet/e-mail system is the property of the municipality and can be reviewed at any time.

## 14. CLEAR DESK AND CLEAR SCREEN POLICY

In order to reduce the risk of unauthorised access or loss of information, FBDM enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers;
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended; and
- Care must be taken to not leave confidential material on printers or photocopiers.

## 15. BYOD (BRING YOUR OWN DEVICE) POLICY

FBDM grants its employees the privilege of using their smartphones and tablets of their choosing at work for their convenience, those devices may not be connected to FBDM network, without written permission from ICT manager. The municipality reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined above.

This policy is intended to protect the security and integrity of the municipality data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

The municipality's employees must agree to the terms and conditions set forth in this policy in order to be allowed to connect their devices to the company network.

## 16. ACCEPTABLE USE

Employees are expected to:

(a) conform to all other appropriate policies and guidelines from the ICT;
(b) Use the network in the way that it is intended to and not wilfully cause any disruptions to the network infrastructure, authorised users or to those given permission by the designated authority which are permitted to use the municipality's ICT facilities;
(c) Not be allowed to disclose any confidential work-related information to any other party, without permission;
(d) Comply with all software licenses and copyrights on their computers;
(e) Ensure that copyright material are not placed, copied or redistributed on the network without the author's or owner's explicit written permission;
(f) May not use municipal ICT equipment for personal financial gains; and
(g) May not change or amend any hardware, software or any other ICT infrastructure without permission.

Employees may use their mobile device to access the following municipal-owned resources: email, calendars, contacts, documents, etc. Those devices should be secured by the means of password or pin.

**RISKS/LIABILITIES/DISCLAIMERS**

The municipality reserves the right to disconnect devices or disable services without notification.

Lost or stolen devices must be reported to the municipality within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

The employee is expected to use his or her devices in an ethical manner at all times and adhere to the municipality's acceptable use policy as outlined above.

The employee assumes full liability for risks including, but not limited to, the partial or complete loss of municipality and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

The municipality reserves the right to take appropriate disciplinary action up to and including termination for non-compliance with this policy.

## 17. ENFORCEMENT

The municipality will not tolerate any misuse of ICT systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use.

Use of any of the municipality's resources for any illegal activity will be subjected to disciplinary process and the municipality will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.