



**JOONDALUP KINROSS JUNIOR
FOOTBALL CLUB
INCORPORATED**

“JETS”

**INFORMATION
TECHNOLOGY
(IT) RULES**

INFORMATION TECHNOLOGY (IT) RULES AND INSTRUCTIONS FOR JKJFC MEMBERS

1. Introduction

This document describes IT rules and instructions to be applied in JKJFC. These standards relate to all JKJFC members who use JKJFC information assets and it is the responsibility of all members to comply with the points described below. Failure to do so may result in disciplinary action.

2. Protecting access to your computer

- Lock your computer when leaving it unattended by pressing CTRL+ALT+DEL and choosing “Lock Computer”.

3. Passwords

- Your User account is personal but not secret.
- Your Password is personal and secret.
- Do not reveal your password to others, including Website/IT administrators
- Do not write down your password anywhere
- Change password immediately if you suspect that it has been compromised.
- Password policy requires changing of passwords every three months or more frequently.
- Recommendation is to use pass phrases rather than passwords

4. Virus protection

- JKJFC computer must have the latest version of the current installed Standard Anti Virus software running. Contact the JKJFC Executive /or their nominee if you suspect you do not have Anti Virus software or it's not updated with latest virus information.
- Be careful when handling new or unknown files in order to reduce the risk of being infected by a virus. Be especially careful when:
 - o Visiting unknown or suspicious websites
 - o Using unknown portable storages e.g. USB memory sticks/drives
- You are responsible for reporting to the JKJFC Executive /or their nominee any occurrence of a virus.

- You must not attempt to remove suspected viruses yourself.

5. Securing your information

- Do not leave your computer unattended and within reach of unauthorized persons when processing sensitive information, or when connected to systems containing sensitive information.
- Do not leave sensitive documents open to the public or in central printers/fax- and copy machines.
- Do not store sensitive data in portable storages e.g. USB memory sticks/drives without encryption
- Storing of data on your computer, you are responsible for taking back-ups of your local hard disk to a portable storage drive..

6. Internet use

- Internet is for JKJFC purposes only and to be used according the standard Internet content filtering software.
- It's not allowed using JKJFC Internet Access to visit sites containing inappropriate content
- Be aware of that all incoming and outgoing Internet traffic through the gateways can be logged and reviewed regularly.
- Do not download suspicious/illegal software or media from the Internet:
 - o Illegal software must not be used on JKJFC computers
 - o Majority of illegal software these days include viruses/spyware/malware
 - o Viruses cause severe security problems e.g. password theft, data theft
- When using Internet, you must be aware of that all communication is done in the name of JKJFC. It can all be traced back to JKJFC. Information retrieved on the Internet must be "handled with care". The integrity of all Internet related information should be questioned.
- Misuse of Internet will result in revoked Internet Access and may also result in other disciplinary actions.

7. E-mail

- You must assume there is a possibility of Internet E-mail to be read by others.

- Be alert when you open messages in which: the sender is unknown, the subject is dubious or if there are attachment that you have not asked for.
- Never disclose your password. If you need to let someone else manage your e-mail, e.g. when you are away contact your JKJFC Executive /or their nominee for redirection.
- JKJFC email must never be redirected to a private mail service e.g. Hotmail, Gmail, etc.
- Be restrictive to give out your Internet E-mail address.

8. Mobile computers / Smart phones

- Think about what you are saying and where, when on your mobile.
- Do not leave your mobile devices unattended in public places.
- Carry your mobile devices as hand luggage when travelling.
- Backup for your mobile devices should be performed regularly.
- If smartphone with push mail is stolen or lost, contact first JKJFC Executive /or their nominee. Then contact your local communication provider for closing the SIM-card.

9. Installation of Hardware and Software

- Do not install hardware or software yourself - Contact your JKJFC Executive /or their nominee for installation approval and advice.
- You are only allowed to use authorized licensed software on JKJFC computers.
- JKJFC computers and data must be used only for Club purposes.
- Unnecessary network protocols and software on the computers should be uninstalled or disabled.

11. How to Handle Incidents

- You must immediately report incidents to the JKJFC Executive/or their nominee.
- Make a note of everything of importance. Make sure you can answer questions about what happened and when.
- Disclose details only to those who need them to carry out their work.