IMMAF IT Communication and Monitoring Policy

Introduction

1. The International Mixed Martial Arts Federation (IMMAF) may provide you with access to various computing, telephone, and postage facilities ("the Facilities") both at the IAAF Office and off site which allow you to carry out designated duties and allow internal and external communication.

2. This Policy sets out IMMAF's policy on your use of these Facilities and includes:

    - Your responsibilities and potential liability when using the Facilities.
    - The monitoring policies adopted by IMMAF.
    - Guidance on how to use the Facilities.

3. This Policy has been created to:

    - Ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring.
    - Protect IMMAF and its employees from the risk of financial loss, loss of reputation or libel.
    - Ensure that the Facilities are not used so as to cause harm or damage to any person or organisation.

4. This Policy applies to the use of:

    - Local, inter-office, national and international, private or public networks (including Internet/intranet and all systems and services accessed through these networks).
    - Desktop, portable and mobile computers and applications (including personal digital assistants (PDAs).

- Mobile telephones (including the use of WAP services).

- Electronic mail and messaging services.

Observation of this Policy is mandatory and forms part of the Terms and Conditions of Employment. Misuse of the Facilities will be treated as gross misconduct and may lead to dismissal.

COMPUTER FACILITIES - USE OF COMPUTER SYSTEMS

5. Subject to anything to the contrary in this Policy the Facilities must be used for business purposes only.

6. In order to maintain the confidentiality of information held on or transferred via IMMAF's Facilities, security measures are in place and must be followed at all times. A personal log-on ID and password is required for access to IMMAF's network. IMMAF reserves the right to override your password and obtain access to any part of the Facilities.

7. You are responsible for keeping your password secure. You must not give it to anyone, including colleagues, except as expressly authorised by IMMAF.

    - In an office environment, always log off the network before leaving your computer for any period of time, in case of hot desking, other members of staff have the right to log on to your computer when necessary.

8. You are expressly prohibited from using the Facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of IMMAF or its clients other than in the normal and proper course of carrying out your duties for IMMAF.

9. In order to ensure proper use of computers, you must adhere to the following practices:

    - Anti-virus software must be kept running at all times.

    - All forms of media storage, (USB's etc.) must be checked by relevant IT/Operations staff before the contents are accessed or stored on IMMAF's network or hard drives.

- Obvious passwords such as birthdays and spouse names etc must be avoided. The most secure passwords are random combinations of letters and numbers.

- when sending data or software to an external party by USB etc. always ensure that the data has been checked for viruses by the IT/Operations staff before sending it.

- All files must be stored on the network drive which is backed up to avoid loss of information.

- Documents must not be stored on your desktop.

- Always log off the network before leaving your computer for long periods of time or overnight.

SOFTWARE

10. Software piracy could expose both IMMAF and the user to allegations of intellectual property infringement. IMMAF are committed to following the terms of all software licences to which IMMAF is a contracting party. This means that:

    - Software must not be installed onto any of IMMAF's computers unless approved in advance by the IT/Operations Department. They will be responsible for establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the computer Facilities.

    - Software should not be removed from any computer nor should it be copied or loaded on to any computer without the prior consent of the IT/Operations Department.

LAPTOP COMPUTERS

11. At various times while working with IMMAF, you may use a laptop. These computers, along with related equipment and software are subject to all of IMMAF's policies and guidelines governing non-portable computers and software (see two paragraphs in software section above). However, use of a laptop creates additional challenges especially in respect of potential breaches of confidentiality. When using a laptop:

- You are responsible for all equipment and software until you return it. The laptop must be kept secure at all times.

- You must not load or install files from any sources without IT/Operations staff inspecting such files for viruses.

- All data kept on the laptop must be backed up regularly in order to protect data against theft or mechanical failure or corruption.

- You must password protect confidential data on disks or on the hard drive to protect against theft.

- If you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the attention of the IT/Operations staff.

- Upon the request of IMMAF at any time, for any reason, you will immediately return any IMMAF laptop, equipment and all software to IMMAF.

- If you are using your own laptop to connect with IMMAF's network or to transfer data between the laptop and any of IMMAF's computers you must ensure that you have obtained prior consent of the IT/Operations staff, comply with its instructions, and ensure that any data downloaded or uploaded is free from viruses.

E-mail (Internal or External Use)

12. Internet e-mail is not a secure medium of communication – it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending confidential information by e-mail this should be sent using password protected attachments.

13. E-mail should be treated as any other documentation. If you would normally retain a certain document in hard copy you should retain the e-mail.

14. Do not forward e-mail messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the e-mail.

15. Your e-mail inbox should be checked on a regular basis.

16. As with many other records, e-mail may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

17. If you are away from the office and use e-mail as an external means of communication you must ensure that the autoreply service is used to inform the sender that you are unavailable. Failure to do so could lead to disciplinary action. If you have any doubt as to how to use these Facilities please contact the IT/Operations staff.

18. Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of the Facilities is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

INTERNET

19. Use of the Internet, or Internet services, by unauthorised users is strictly prohibited. You are responsible for ensuring that you are the only person using your authorised Internet account and services.

20. Downloading any files from the Internet using the computer Facilities is not permitted. If there is a file or document on the Internet that you wish to acquire, contact the IT/Operations staff to make arrangements for it to be evaluated and checked for viruses. It will be at the discretion of the IT/Operations staff on whether to allow such download.

21. Posting information on the Internet, whether on a newsgroup, via a chat room or via e-mail is no different from publishing information in the newspaper. If a posting is alleged to be defamatory, libellous, or harassing, the employee making the posting and IMMAF could face legal claims for monetary damages.

22. For the avoidance of doubt the matters set out above include use of WAP facilities.

MONITORING POLICY

23. The Policy of IMMAF is that we may monitor your use of the Facilities.

24. IMMAF recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the Facilities.

25. IMMAF may from time to time monitor the Facilities. Principle reasons for this are to:

- Detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies.

- Ensure compliance of this Policy.

- Detect and enforce the integrity of the Facilities and any sensitive or confidential information belonging to or under the control of IMMAF.

- Ensure compliance by users of the Facilities with all applicable laws (including Data Protection), regulations and guidelines published and in force from time to time.

- Monitor and protect the well-being of employees.

26. IMMAF may adopt at any time a number of methods to monitor use of the Facilities. These may include:

- Recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content.

- Recording and logging the activities by individual users of the Facilities. This may include opening e-mails and their attachments, monitoring Internet usage including time spent on the Internet and web sites visited.

- Physical inspections of individual users' computers, software and telephone messaging services.

- Periodic monitoring of the Facilities through third party software including real time inspections.

- Physical inspection of an individual's post.

- Archiving of any information obtained from the above including e-mails, telephone call logs and Internet downloads.

27. IMMAF will allow third parties to monitor the Facilities.

28. IMMAF may be prohibited by law from notifying employees using the Facilities of a disclosure to third parties.

General Guidance

29. Never leave any equipment or data (including client files, laptops, computer equipment, mobile phones and PDAs) unattended on public transport or in an unattended vehicle.

30. When using e-mail or sending any form of written correspondence:

- Be careful what you write. Never forget that e-mail and written correspondence are not the same as conversation. They are a written record and can be duplicated at will.

- Use normal capitalisation and punctuation. Typing a message all in capital letters is the equivalent of shouting at the reader.

- Check your grammar and spelling.

- Do not forget that e-mails and other forms of correspondence should maintain the high standards expected by IMMAF. Where applicable you should use formal headings and introductions such as "Dear… and "Yours sincerely" etc.

Observation of this Policy is mandatory and forms part of the Terms and Conditions of Employment. Misuse of the Facilities will be treated as gross misconduct and may lead to dismissal.