APF INFORMATION TECHNOLOGY
ACCEPTABLE USE POLICY v1.0-JULY 2022

CONTEXT AND PURPOSE

This policy covers employees, volunteers and members of the Australian Parachute Federation Ltd. It covers hardware and software that is owned or managed by APF.

It also covers hardware that appears on the APF Equipment Register but is used by Area Councils for carrying out their delegated roles under the Council Charter.

The responsible person for the operation of this policy is the CEO, who may choose to consult with relevant experts in carrying out this role.

AUTHORISED USE

The systems are primarily an APF tool, to be used for APF purposes by staff, volunteers and members.

- In the case of staff, this includes uses relevant to their employment with APF
- In the case of volunteers, this includes uses relevant to their unpaid roles and responsibilities with APF
- In the case of members, this includes uses only for the purpose for which they have been given access to the systems

PERSONAL USE

- Any personal use of APF equipment and systems should be incidental and not interfere with the user's role within the Company, the work of others or the operation of the systems.
- However, unreasonable or excessive personal use is not permitted. For example, the systems must not be used to conduct a personal business or private commercial activity, gamble, transmit objectionable material or carry out excessive and regular research into topics not related to APF aims and objectives.

CONDITIONS OF ACCESS

It is a condition of access to the systems that users must agree to comply with all published APF policies including those relating to Code of Ethics or Code of Conduct:

Staff and volunteers with APF email/intranet accounts

- are presumed to be responsible for all activities undertaken using their accounts
- must take reasonable steps to keep their account secure
- must choose a password that cannot easily be guessed or predicted

- must not share their password with anyone else or record their password in obvious locations
- must change their password regularly (and immediately if it becomes known by another person)
- must not permit other persons to use their account (other than through an email proxy arrangement or unless approved in advance by the CEO
- must log out or lock their computers whenever they are left unattended
- must protect the security of data held on APF owned mobile systems (eg phones, laptops, USB drives and other storage mediums), including by maintaining reasonable virus control measures where possible
- must not connect unauthorised devices to the network, either via software or hardware that makes this possible (eg attaching a personal computer or external storage device)
- must not use abusive, profane, threatening, racist, sexist, or otherwise objectionable language in any message
- must not access, send, receive, store, or print pornographic, racist, sexist, or otherwise discriminatory, or objectionable material
- must report actual or suspected security breaches to the CEO as soon as possible
- must not defeat or attempt to defeat security restrictions on systems and applications
- must not remove or disable antivirus and other similar client security agents without approval from the CEO
- must not use or install unauthorised or unlicensed software
- knowingly propagate or disseminate malicious software of any type
- must not attempt to defeat, override or bypass the two-factor authentication system in use for APF account holders.

Privacy

Users must deal with personal information in accordance with the APF privacy policy

Staff and volunteers with APF email accounts:

- use the systems on the understanding and condition that their use on APF accounts may be monitored
- acknowledge and consent to APF's right to access, monitor, filter and block electronic communications created, sent or received by any user using APF systems
- acknowledge that staff and volunteer access is provisioned when commencing their roles and access will be removed in a timely fashion after those roles cease

Subject to the approval and at the discretion of the CEO or other authorised person and for compliance with applicable legislation, APF reserves the right to (without notice):

- intercept, access, monitor and use electronic communications created, sent or received by users of the APF systems in any manner determined by the APF (including as records of evidence in an investigation or in response to other actions such as audit, litigation, criminal investigations or freedom of information requests)

- monitor the use of any device or terminal
- inspect any data residing on any APF-owned resource (regardless of data ownership and including personal emails and other personal communications and data stored in personal file directories)
- capture and inspect any data in any computing infrastructure owned by APF
- delete or modify any data in its network
- re-image its desktops and laptops as and when required
- apply filtering systems to the network that limit use and activity by preventing communications based on size or content

For example, communications may be blocked if they are suspected:

- to contain unlawful material
- to be unsolicited commercial electronic messages within the meaning of the Spam Act 2003 (Cth).

Email

APF supplies email accounts to staff and to some volunteers. These accounts must be used in preference to personal email accounts for all APF business and operational matters. Emails sent from these accounts are directed only to the recipient(s) and may not be shared, by the recipients, with others either through forwarding or posting on social media.

APF licenses and manages the use of specialist judging software (In-time). The approved use of that software is for the conduct of regional and national APF endorsed skydiving championships as well as the training of judges to judge at those particular skydiving championships. Any usage outside of what is proscribed above is prohibited without the express written permission of the CEO.

Member website access

Members are given the privilege of an APF website login for the purpose of managing their personal information, voting in Director elections, and managing their interactions with a range of APF services. Use of this login for any purpose other than its intended use is expressly prohibited. Should any unauthorised use be detected, the CEO may direct that the privilege be removed either for a period of time, or permanently. Should access be removed, APF will provide alternate means of carrying out the functions normally done through the member login for the affected member during the time they are denied use of their website login. Member website logins will be removed if membership fees are not paid. This is not applicable to Life Members or Honorary Life Members.

Social media

APF and Area Councils may have a social media presence of a nature that allows APF members and/or members of the public to make posts that may be viewed by others. APF members will be held responsible for the content of their posts on APF or Area Council social media and may be subject to disciplinary action for inappropriate posts.

Examples of inappropriate posts include posts that may be interpreted (in the eyes of APF) as defamatory, offensive, derogatory, homophobic, racist, sexist, pornographic, or of a nature that may be seen as intimidatory towards another member. Posts that are seen to promote illegal activity or activities that may be in breach of the APF Operational Regulations are also subject to removal.

Social media posts described in the previous paragraph may be removed at any time by the relevant moderator without notice or recourse.

Members who make inappropriate social media posts to non APF platforms may be subject to APF disciplinary action relating to the act of bringing our sport into disrepute.