

## **BL003.00**

### **IT, Web Site and Email Procedures**

#### BL003.01 Information Security Policy

##### (i)Introduction:

Computer information systems and networks including the IPDA Web site and any other hardware facility, henceforth described as “IT”, are an integral part of the Association’s activities. The Association depends upon the efficient performance of the IT to provide a service to and communicate with Association members and the general philatelic public.

The Policy and directives contained in this Procedure have been established in order to:-

- protect our investment in the human and IT resources that we use;
- safeguard the information contained & stored in the IT;
- reduce business and legal risk;
- protect the good name of the Association.

##### (ii)Contents:

The topics covered in this By-Law include

- introduction;
- violations;
- the IT;
- unacceptable use;
- downloads;
- Computer viruses;
- Spyware and Adware;
- access codes and passwords (if required);
- physical security;
- copyright and license agreements;
- acknowledgement of information security policy.

##### (iii)Violations:

Violations may result in serious consequences for the Association, such as, the disruption or breakdown of the IT or its ability to securely store valuable and private

information and provide member services. Failure to observe these guidelines may result in action being taken against anyone found to be causing a disruption or breakdown, depending upon the type and severity of the violation and whether it causes any liability or loss to the Association or a member or a visitor to our web site.

- Disclaimer.

Whilst the Association will take all possible steps to maintain and use the IT in an efficient, legal and ethical manner it will not accept responsibility or liability for actions of members, or other people, who do not use the IT in the manner required by this Policy or who use it illegally.

(iv) Administration and Responsibility:

The IPDA Web Master is responsible to the Board of Directors for the administration of this Policy. In addition, he is required to report to the Board any violation of the policy and its directives.

The Web Master, supported by the Board of Directors will:

- ensure that all members are aware of and comply with this Policy;
- create appropriate performance standards, control practices, and procedures necessary to provide adequate assurance that all members will observe this Policy

(v) The IT:

The internet is a very large, publicly accessible network with millions of users and organisations worldwide and is filled with risks and inappropriate material.

The Association does not provide direct access to the worldwide internet for the benefit of members apart from the publicity offered by its IT facility and member's advertisements. Conversely, to ensure that members are responsible and productive IT users and to protect the Association's interests, the following Policy and guidelines are provided for using the IT.

Members using the IT for philatelic purposes for or on behalf of the Association, must ensure it is used in a responsible, effective, ethical and lawful manner, whenever they;

- use web browsers to obtain information from commercial web sites;
- access databases for information;
- use e-mail services whether owned by the Association or themselves.

(vi) Unacceptable use:

Members must not use the IT for unlawful unethical purposes or harmful to the Association. Examples of unacceptable use are:

- sending or forwarding chain mail to or between members, i.e. messages that contain instructions to forward its contents to others;
- transmitting any content that is offensive, harassing, untruthful or fraudulent;
- conducting a personal business on the IT, i.e. the Association's IT, except where the Board of Directors has given permission.

(vii)Downloads:

Members will be able to download information from the Association's IT facility, i.e. that part of the web site which is open to the public, and from the Reference Library and other specified parts of the member's area. Members may use e-mail addresses belonging to other members to communicate with each other, but may not sell or pass any e-mail addresses without permission (see Rule 16.2 Of the Constitution – Custody of Records and Privacy). A member may request that their e-mail address and personal information is not used for any purpose other than the normal conduct of Association business with members.

Members using or quoting the Association's IT are required to ensure that:

- all communications are for professional reasons and on behalf of the Association;
- he accepts responsibility for the content of all text, audio, images, banners or advertisements he places on the IT or send through the IT to other persons and organisations;
- he will not use the Association's copyright material without permission;
- he is familiar with and will apply all applicable policies and procedures dealing with the security and confidentiality of Association records;
- he will run a virus scan on any executable file received through the IT or sent to it.

(viii)Computer viruses:

The Webmaster shall:

- install and maintain appropriate antivirus software to protect the Association's IT and any computer hardware used to operate the IT;
- respond to all virus attacks, destroy any virus detected and record all incidents.

Members are;

- expected to do likewise on their computer systems and to advise the Web Master and all other members when they experience similar attacks which may have been passed to other members and the Association's IT with the exchange of emails;
- not use diskettes of unknown origin;
- immediately power off their IT hardware if they discover a virus has invaded their system and advise all other members and the Web Master accordingly;
- take steps to destroy any virus that has invaded their IT hardware and advise all other members and the Web Master when this successfully been accomplished.

(iv)Spyware and Adware:

The Web Master will:

- install and keep up to date appropriate anti spyware and adware software on all IT operating the Association's systems;
- respond to all reports of spyware installation, remove spyware modules, effectively restore the system and record all incidents.

Members are:

- expected to do likewise with their IT hardware and to advise all other members and the Web Master whenever they experience a case of spyware which may have been attached to email messages exchanged between them.

(v) Access codes and passwords:

Where the Association introduces the use of passwords, or uses codes (e.g. to enter the IPDA Chat Rooms and member's only sections of the Association's web site) to restrict entry and protect from unauthorised access, the Web Master shall maintain a list of administrative access codes and passwords and keep this list in a safe place, off site.

The Web Master will change all passwords at least once every 180 days and shall use passwords that are randomly generated and not easily guessed by others.

Members who are given passwords and/or codes to access the Association's web site and Chat Rooms shall be responsible for all IT transactions that are made using their ID's and passwords or codes.

Members shall :

- not give their ID or password or code to any other person
- ensure that where they invited to generate their own password that it is done so as not to be easily guessed by others;
- keep their passwords in a safe place;
- should log out when leaving their workstation for any extended period of time;
- should not attempt to access any other member's account without the owners permission.

(vi)Physical Security:

The Association will take whatever steps are needed to protect its IT, software, data, and documentation from unauthorised use or access, theft and environmental hazards.

The Web Master, Office Bearers and members using the Association's IT and when dealing with information that belongs to the Association, or a member or a third party shall;

- store all diskettes out of site when these are not being used;
- lock up confidential and sensitive data;
- keep diskettes and documentation away from environmental hazards such as direct sunlight, excessive high or low humidity, magnetic fields, smoke, extreme heat or cold ;
- that file servers are protected by an uninterruptible power supply (UPS) and power surge suppressors;
- ensure that any hardware used by the Association is provided with adequate protection against over heating by using cooling fans and other devices.

(vii)Copyright and license agreements:

It is the Association's Policy to comply with all laws regarding intellectual property.

- Legal reference: The Association, its Officer Bearers and members are legally bound to comply with all proprietary software license agreements entered into. Non-compliance may expose the Association and the responsible Officer Bearers or members to civil action and/or criminal penalties;
- Scope: This Policy applies to all software owned or used by the Association, Licensed to the Association, or developed using the Association's physical and human resources or vendors;
- The Web Master will be responsible for maintaining records of software licenses owned by the Association and will periodically, at least twice

annually, scan the Association's IT facility to verify that only authorised software is installed.

(viii) Acknowledgment of this Information Security Policy

All members are expected to keep themselves up to date with the requirements of this Policy.

The Association's Membership Secretary shall include in all letters of welcome to new members a sentence drawing the new member's attention to this Policy.

The Membership Secretary will also ensure that a reference to this Policy is included in the Application for Membership (Form BL007.01) which requires applicants for membership to understand that by making their application to become a member of the Association they have actually read and accepted the Code of Ethics and this Policy.

*(NOTE: A notice drawing all members attention to this Policy will be placed on the Association's web site and published in the Member's Newsletter – April 2006.)*