



PRETORIA PHOTOGRAPHIC SOCIETY

DATA PROTECTION POLICY

1. BACKGROUND

This policy is prepared and maintained in terms of the Constitution of the Pretoria Photographic Society (PPS). It describes the measures the PPS will take to protect the data of the PPS and its members, and also the limitations of such protection. The term data includes the protection of images and personal data of members.

2. PROTECTION OF DATA ON PPS COMPUTERS

- (a) PPS will install similar levels of virus and malware protection on its computers as found in the home situation. This includes free versions of such software.
- (b) Protection software will be updated on a regular basis, at least monthly.
- (c) Operating systems will be updated regularly, at least quarterly.
- (d) Backups of PPS data will be taken at regular intervals, at least monthly. Such backups will be protected in the same way as data on PPS computers.
- (e) PPS Computers are to be used only for PPS purposes, in order to limit the exposure to potential attacks.

3. CODE OF CONDUCT

- (a) All members who handle the data of members shall formally accept the Code of Conduct, detailed in the Annexure of this policy. It is specifically noted that this code of conduct prevents distribution of images and personal data outside of PPS and requires personal data not to be distributed in tabular form that can easily be copied.

4. USE OF EXTERNAL SOFTWARE APPLICATIONS

PPS uses external software applications, such as Irfanview and PhotovaultOnline. PPS also has a web presence in the form of a website and Facebook page. Other applications are possible in the future.

- (a) Where such applications store members' images, PPS will obtain and circulate to members the degree of protection provided by such applications.
- (b) If PPS places images on publicly accessible applications, it will protect the images by watermark, low resolution or prohibition of copying.
- (c) If members place images on publicly accessible applications, they are responsible for protection measures.
- (d) Where there is a large body of stored images, such as in PhotovaultOnline, the policy of that application will be obtained and communicated to members.



5. RETENTION OF IMAGES AND THEIR COPYRIGHT

- (a) The images held by PPS have been a valuable source of backup for members who have lost their own images. For this reason, PPS retains all images on its computers and associated backups.
- (b) The copyright of all members' images remains with members.
- (c) However, they grant PPS the non-exclusive right to use these images in the various competitions arranged by the Photographic Society of South Africa (PSSA); and other uses with the permission of members.

6. LIMITATION OF LIABILITY

The management and operation of PPS are undertaken by unpaid volunteers, who are also not data protection specialists. For this reason, PPS and its members indemnify the committee, the projection team and any member authorised to handle their images from any financial claim for the misuse of images or personal data.

7. APPROVAL

This policy was approved at the Annual General Meeting dated 15 August 2017 and continues in effect until superseded. It supersedes all previous versions of this policy.



Code of Conduct

Pretoria Photographic Society: Committee and Projection Team members.

I, _____
undertake to comply with the Data Protection policy of the Pretoria Photographic Society (PPS)
dated 15 August 2017. In doing so, I will:

1. Recognise that the copyright and ownership of images always reside with the author and undertake not to take any action that diminishes the authors' rights.
2. Never distribute personal information of members outside of the PPS, except for the contact details of a person designated to receive enquiries from the public, normally the President or Secretary.
3. Never distribute images of members outside of the PPS, except for
 - a. Posting of images on the PPS website and social media as authorised by the committee.
 - b. Entry of images into the PSSA competitions approved by the committee. Initially this represents Interclub Competitions and Monthly Club Winners' competitions.
4. Never distribute the entire membership list, inside or outside PPS, in a tabular machine-readable form such as Excel or Word tables without the specific permission of the committee for a nominated purpose.
5. Protect the integrity of the computers used by PPS by installing and keeping current (i.e. at least monthly) the virus and malware protection software approved by the Committee. Initially this software is Windows Defender and Malwarebytes (free versions).
6. Regularly update the operating systems of PPS computer(s), at least every three months and immediately on becoming aware of major new threats.
7. Alert the committee to any suspected threat to the data on the PPS Computer(s).
8. Avoid using the PPS computer(s) for any purpose other than the those of the PPS.
9. Evaluate major changes to external software for potential threats to the integrity of members' personal data and images.
10. Make regular backups of the user data on PPS computer(s), with such backups to be kept physically separate from the computer(s) and subject to the restrictions on distribution as listed above.

Signed:

Date: