**W&CCC Data Security Procedures**

V1.0, Mark Wycherley, 13th April 2018.

# Introduction

Committee members must follow the procedures outlined herein that affect their roles.

Committee member nominees must also familiarise themselves and be comfortable with the procedures for their nominated role before standing.

In reading these it should be understood that these are non-exhaustive and should also be taken as best practice guidelines.

# Definitions

The Club holds 5 classes of personally-identifiable data on current and past members:

1. **Sensitive Club Data** (data that needs be handled via very strictly-controlled possession and distribution, primary encountered examples below only):

* Membership Database containing members’ names, members’ photographic accreditations, members’ home addresses, members’ phone numbers, members’ e-mail addresses, members’ subscription payment information, members’ acceptance or otherwise of information sharing to members’ website. The database is singly owned and distributed by only the Club Secretary. Each version issued has a unique filename and is password protected. The password is then shared to recipients by phone call or text (i.e. not via e-mail unless obfuscated).
* Club membership waiting list containing names and contact details of enquiries and ongoing applications. Held only by the Club Secretary and Chairman.
* Membership Application Forms (paper). Held by only the Club Secretary.
* All-members e-mail distribution list. Held only by the Club Secretary.
* Member’s IP addresses and access logs as recorded for all website accesses. Logged by the website server and accessible by only those with website Admin rights.
* Website backups.
* Electronic copies of member’s membership cards. Held by the Club Secretary.
* Letters in support of member’s PAGB assessments. Held by the Club Secretary.
* Miscellaneous private e-mail dialogues and enquiries between members and committee members regarding operations of the club.
* Any investigations into rule breaches.
* Any accident/incident reports or insurance claims concerning members.
* Any club bank account statements showing payment and income information.

1. **Privileged Club Data** (can be given to and retained by any committee member on need-to-know basis or in the course of specific committee duty):

* Official committee meeting minutes. Any personal notes or recordings made during committee meetings. NB Some topics discussed at committee meetings may be regarded as Sensitive and the data pertaining to them need be classified as such.
* Members’ competition images/AVs – including any metadata within (personally identifiable information may be within image metadata).
* The club competition image database and associated spreadsheets, referencing members’ image titles, competition scores, and league positions.
* Photographs of members taken at Club events.
* Original high-resolution photographs of members taken for posting the list of members on the website.
* Documents created by other committee members about the club and its operations. Includes analytical documentation supporting committee actions or decisions.
* Club insurance policy and schedule information.
* Club bank account and financial information – over and above that shared with all members at the AGM. May also be shared externally in the support of grant applications.
* Information relating to any complaints, concerns, or investigations into members.
* Booking information relating to speakers or judges.
* Members’ questionnaire responses as logged by the website.
* Club meeting attendance lists.
* Club event registration and attendance lists, including temporary set-up and information sharing e-mail distribution lists.
* Competition entry image database, including all images or selected high-scoring images, and intermediary competition software files.
* Club laptop backups.
* Attendance records of club outings, holidays, and events.

1. **Privileged External Data** (can be given to and retained by only those committee members needing to use the data in the course of their role in organising club activities):

* Images/AVs given to the club by members of other clubs for use in inter-club competitions – including any metadata within.
* Presentations, images, and notes when given to the club for Speaker talks.
* SPA, SCPF, and PAGB handbooks, giving list of Judges and Speakers names and contact information for them.
* SPA, SCPF meeting minutes where shared into the Club’s Committee.
* Club laptop backups, where containing External Data such as inter-club competition images from other clubs.

1. **Common Club Data** (viewable and locally saveable by all members on the club members website or in hard copy of club magazine or distributed at or prior AGM):

* Members’ image files (including original metadata within the file from submitting member).
* Members’ scores and league positions.
* Records of trophy awards (member names).
* Photos of members taken at club events.
* Head shot photos of members as used in website members list.
* Members’ usernames and avatars where used on the members website.
* Members’ comments on website.
* Members scores and comments on the website. The scores are not individually attributed as seen by other members but the comments are.
* Published copies of club magazine.
* Annual Club Accounts.
* AGM and EGM agenda and minutes.

1. **Public Club Data** (made available on public website):

* Committee Members’ names and roles (contact e-mail addresses are aliased).
* Selected Committee Members’ headshots.
* Season Programme with judges’ names, speakers’ names and associated talk titles and competition name.
* Member’s images in the image attractor rotator. Images are not specifically attributed and are provided voluntarily. A general statement asserts copyright to the individual author. Reduced resolution versions and metadata has not been included.

# General principles of data retention

The club regards its history as a strong aspect to its heritage and prestige. As such in principle it retains some members’ data in perpetuity (such as images, image scores, awards, membership period, committee membership, website comments). Historical archive information should pass from a retiring Committee Member to their successor in its entirety, thereafter being deleted by the retiring Committee Member. Some data and archives may periodically be pruned by the holding Committee Member under the guidance of the Committee. In general though, the Club regards that any data generated as a consequence of a member’s interaction with the Club is part of the Club’s history and records and therefore will be retained.

# Procedures and obligations

## For all Committee Members:

General procedures:

* Must agree to share openly their e-mail addresses and contact phone number(s) with each other and with all members of the club (via the website).
* Keep Privileged Club Data secure at all times. Data can be kept on home computers, but the data must be kept in separate folders from personal data or from any data related to other activities the Committee Member may be active in. Any backups must be equally secure – backups drives/folders should be password protected.
* Privileged Club Data should not be placed on cloud backup up or sharing servers unless password protected as data files (or in strongly password protected folders).
* Not share Privileged Club Data outside of the club – including to other clubs, federations, etc.
* Pass any relevant Privileged Club Data onto their successor.
* Delete all their own copies and own backups of Privileged Club Data after handover to their successor on leaving their position.
* Not share the Privileged Club Data or any part of it with other club members.
* Keep any paper copies of Privileged Club Data secure (in locked filing cabinets for example).
* Must only send all-member e-mails via the Club Secretary who will use the formal all-member list in bcc format. If addressing a subset of members (for example in setting up a club event), then can originate the mail by oneself, but only use bcc to each member (unless otherwise agreed or the attendee list is published for the purposes of the event for car-sharing, etc.).
* Keep club e-mails separate from personal e-mails (separate folders within the mail-client, etc.).

When handling Sensitive Club Data:

* Never forward or onward share to anyone any Sensitive Club Data or part of it without the express permission of the Club Secretary or Chairman. Under no circumstances should any or all of it be shared with other members or anyone outside of the club.
* Not adapt, alter, or add to any of the Sensitive Club Data or its containing document without the express permission of the Club Secretary.
* Not extract any part of the Sensitive Club Data other than member’s names and e-mail addresses (and then only for example for the purposes of administering competitions or administering the club website).
* Not copy the sensitive data and repurpose in another format without the express permission of the Club Secretary.
* Not use any part of the Sensitive Club Data for anything other than club business. This includes using for any kind of 3rd party marketing regardless of whether related to photography or not.
* Delete any copies of Sensitive Club Data when requested by either the Club Secretary or Chairman.
* Delete any copies of superseded Sensitive Club Data – unless securely retained with the knowledge of the Club Secretary.

## For Club Secretary and Chairman:

In addition to above, procedures for Club Secretary and Club Chairman regarding Members Database and Waiting List:

* May only share elements of the Members Database (or Waiting List) with other members of the club provided that the members (or prospective members) whose data is being shared have granted permission that the pieces of information as requested should be shared with the receiving member or members only for the purpose they permit and in the form they permit.

When enacting right to be forgotten requests from departing members:

* + Ensure that all Committee Members holding Sensitive Data pertaining to the ex-member delete all such Data. Update and reissue Membership Database as needed.
  + Ensure that Privileged Data such as the requesting ex-member’s headshot is removed from the club website.
  + Ensure that departing member’s access to the club website has been withdrawn.
  + Explain to departing member that all their other data (for example their images, their image scores, league tables with their position within, their website comments, etc.) will be retained, both to keep all other data integral and also for historical and archive purposes. A member cannot leave and expect us to re-write the documents (for example competition league score sheets) as though they were never in the club.

When fulfilling a request by a member to view their data held by the Club:

* + Extract the relevant line from Membership Database and show that.
  + Refer them to our Data Protection Policy and this implementation document; walk them through the various data on them by way of example where necessary.
  + Show any spreadsheets with records of competition participation: image titles and scores, etc.,

## For Club Webmaster:

In addition to above, then when a member leaves:

* Delete departing member’s account from website.
* Delete the member and headshot from the members’ gallery. Comments, images, scores, league positions, and all other data pertaining to the ex-member can remain (citing historical and archiving reasons).

In general administration of the Members website:

* Ensure that members do not share personal data (addresses, phone numbers, etc.) about themselves or other members (Committee Members details are published elsewhere and those should be linked to and not repeated). Delete any case where member’s details are shared.

# Management of the Club Facebook Group

The Club Facebook group shall be manage thus:

* The Chairman and Webmaster will have Admin rights
* Only members and past members shall be allowed as members.
* Posts should be encouraged to only relate to things of interest to club members, but can be posted by any member of the FB group.

# Management of competition image database

In the course of the Club’s normal competition activities it gathers a database of higher scoring images that are then used as candidates in external competitions. The Club’s image database is saved on portable external hard-drive and on DVD. The master copy is held by the external competition secretary. The database is classified as Privileged Club Data and should follow the procedures for data of that class.

It is considered at the member’s own risk if they choose to include personally identifiable metadata within their images. The club does not delete metadata from member’s images as this could interfere with other copyright and licence assertions made by the member. Refer to the separate section on metadata.

[ Do we have any systematic process for images which are entries but are not high-scoring?? I know all PDI comps entries are left on the club laptop, but I am not sure this is part of any real intent. Image files should be kept if needed in any rule infringement investigation. ]

# Use of members’ images in inter-club competitions

Members agree in the Membership Registration Form that their images may be used to represent the Club in external competitions. If the member agrees, then their image may also go on to represent the Federation.

There may be separate agreements between the Club and the receiving organisers as to what may be done with the image and the data contained therein.

It is considered at the member’s own risk if they choose to include personally-identifiable metadata within their images. The club does not delete metadata from member’s images. Refer to the separate section on image metadata.

# Security of the Club laptop

Security of the club laptop:

* Should have password-protected account for club use. All club data and images should be kept within that account.
* Should only have images and scores on it, and no other Privileged club documents.
* Must never have Sensitive club data on it.
* Any Privileged External Data should be removed at the start of each season.
* Should run anti-virus software.
* Should be kept up-to-date with latest version of operating system.
* Should be kept up-to-date with latest versions of competition and other software used by the club, provided that those latest versions are fully compatible with prior versions and with the needs of the club.
* Should not have software unrelated to club business installed on it.
* Should be backed-up regularly with complete disk image for recovery in case of crash.
* Should be switched off when not in use, and not left unattended.
* Should be disconnected from external Wi-Fi or LAN except during file-transfer or software updating.
* Should not be used by anyone unless under the supervision of a Committee Member.
* Should not be left in parked vehicle unless within locked boot and out of sight.

# Precautionary note regarding image metadata

Images submitted to the club may contain personally-identifiable information in their embedded metadata. This could be the member’s name, address, phone number, personal website address, GPS location, body serial number, lens serial number, document ids, Adobe application information, and other freeform information (keywords, face detection markers, etc.).

If the metadata is there, it is readily readable with commonly-available applications.

The club will (and should) not remove metadata as it may have been added and specifically pertain to copyright and licensing assertions the member may wish to make.

It should be noted that the Club does not require any metadata to be in the images. Whilst the Competition Rules require that the Member does hold copyright to the submitted image, it does not require that that copyright is asserted in any copyright notices in the image file itself.

It is assumed that the member grants the club the license to use the image as an entry on the club’s behalf in interclub competitions. The club asserts no right to modify or create derivative works – any change to the image must always be done by the original photographer – including any modifications to the metadata content.

It is therefore considered at the member’s risk if any personally-identifiable metadata exists in their image files.

The club also does not check for commercial usage license or privacy factors pertaining to the subject matter. The Club Competition Rules outline more concerning licensing and copyright.

# Competition Trophies and Awards

The club owns trophies, shields, plates, and other awards that may be etched or marked with recipient’s names. The trophies may also be named after a past member. No action need be taken regarding those namings or recipient etchings when any recipient leaves the club; these can all be regarded as being part of the core history of the club.

# Procedures in case of breach

If any committee member becomes aware that a data breach has occurred then they should in the first instance inform both the Chairman and the Club Secretary of the nature and time of the breach. The Chairman and Club Secretary then need determine the appropriate action.

It is unlikely that any breach would warrant notifying any outside body (such as the ICO) as the Club does not gather and retain information which in any way affects an individual’s rights and freedoms.

# Appendix – tabular summary

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Retention period, and reason.** | Perpetuity as a historical record of club membership | Perpetuity as a historical record of club membership | Continuously updated with current members' e-mail addresses | Perpetuity (also retained at bank) | Perpetuity | At least 3 years, as evidence members have accepted Terms and Conditions in case of any claim against the Club. Longer if there is an active Claim | Perpetuity | Perpetuity | Ad-hoc, but maybe perpetuity | Indefinitely | Perpetuity as a records of club activities | Rolling 12-months | Indefinitely, unless requested to remove it | Ad-hoc | Ad-hoc |
| **Security** | Kept in locked premises (the home of the Club Secretary) | Microsoft Excel Spreadsheet, password protected | Secure accounts, used as bcc only | Kept in locked preimises (the home of the Treasurer) | Club secretary hold master copy and copies are with all committee members | Committee members to delete copy after review | Kept in locked premises (the home of the Secretary) | To include no personal data, only include names as absolutely necessary | Kept in locked premises (of the event organiser) | Limited circulation for general image entries. Higher-score images may be placed on club members' website | Committee members personal computers | Available only to website Admins (password protected) | Data is backed up on to an encrypted remote site | Data is backed up on to a encrypted remote site | Committee members computers only |
| **Processing** | Membership Renewals, Copying into Membership Database Spreadsheet | Used as membership database of paid members | None | Correlation into Membership Database to ensure up-to-date record of payments | Information is not processed, just recorded. | Shared with committee members for review, and included in monthly meeting minutes. Information may be shared with Insurance Company in the event of a claim | No processing | No processing | No processing | Possible EXIF and other metadata or image content checking in the event of a query regarding rule compliance. | Score summation, ranking for league positions | Occasional checking for site design optimisation purposes | No Processing | No Processing | Determination of travel distance to club |
| **Who its shared with** | Treasurer | Treasurer, Chairman, Webmaster, other Committee Members only on need-to-know basis | Chairman | No-one | Committee Members | Committee members via the committee meeting minutes | Chairman | All Members | Event manager and Club Secretary | Competition Secretaries, hosts of external competitions, members website | Committee. In summary form presented as league tables to all club members | No-one | Everyone | Club Webmaster | Ad-hoc (information is primarily sourced from Federation handbooks) |
| **Personal Information** | Names of members, photographic accreditations, home address, phone number(s), e-mail address, acceptance of rules, agreements regarding use of images | Names of members, photographic accreditations, home address, phone number(s), e-mail addres. Includes also recent past-members. | e-mail address (may include readable/deducable name) | Names, dats and amount of payment if via bank trasnfer | Members attending meetings, other Member names, activities, and actions may be recorded | Specific details that may include health information | Member's name, proposer's and seconder's name | Any name that may be mentioned, apologies, committee member nominations, etc., | Name, e-mail address and mobile number | As included by member | Name, any photographic accreditations, image score, any title awards | Username, IP address, browser and OS capabilities | Names, image metadata | Names, image metadata | Speaker and judge names, home address, e-mail addresses, and telephone, mobile numbers |
| **Format** | Registration Forms (paper) | Microsoft Excel Spreadsheet | Google cloud | Printout, pdf | Microsoft Word File | e-mail | Paper form | Microsoft Word File | Hard copy and e-mail | JPEG files with contained metadata | Microsoft Excel, pdf | Retained within site's database and file logs | Hosted on the internet by various organisations. | Hosted on the internet by Club's Internet Service Provider. | e-mail and other documents |
| **Owner – who maintains and looks after it** | Club Secretary | Club Secretary | Club Secretary | Treasurer | Club Secretary | Chairman or other | Club Secretary | Club Secretary | Varies - Designated event manager | Competition Secretaries | Competition Secretaries | Webmaster | Club Webmaster | Club Webmaster | Competition Secretaries, Programme Secretary |
| **Data Source** | Members | Electronic record of membership registration data | Electronic record of membership registration data | Bank | Committee Meeting | Member / investigating committee members | Members | All Members | Attendees for events | Members | Members, Competition Secretaries | Website activity, logins, page-fetches | Members, Competition Secretaries, and Club Webmaster | Club Webmaster | Internal and External Competitions Secretaries, AV Group Leader, Programme Secretary |
| **Why we need it?** | To identify as a current member, their contact details for membership communications, and evidence of their acceptance of T&Cs | Membership database | For circulating all-member e-mails | Cash-flow control of club | A formal record of reporting and decisions. | To comply with Health and Safety | For annual Committee Member elections at AGM | To comply with the Club constitution | So we can administer you as an event attendee | So you can enter competitions | Recording of competition entries and associated judge's score | Recorded by website for access analysis | To share updates to members, and help promote the Club, historical records for the Club | For the purposes of disaster recovery | To build the club season programme and run competitions |
| **Data Title** | Membership registration forms | Current Membership database | Membership e-mail distribution list | Bank statements | Committee meeting minutes | Accident / incident records | Committee Member nomination forms | AGM minutes | Event registration forms | Competition image entries | Competition Score sheets | Members' website access logs | Internet published Photos, Competition Results and News articles | Backup of Internet published Photos, Competition Results and News articles | Speaker and judge booking information |