Bromley & District BSAC Branch (0026): Data Handling Protocol for Committee Members & Other Data Processors

Introduction

This document is designed to summarise how to handle members' personal data within the club. Please read it in its entirety before accessing or processing any personal data. Ideally this should be one of the first documents you read when taking on your role.

The club data controller is the membership secretary. All other committee members are classed as data processors and answer to the membership secretary. If you have any questions, they can be contacted at membership@bromleydivingclub.com.

Highlighted in blue are action points. You should make sure these tasks are complete before handling any personal data. Important warnings are denoted by red.

For the purposes of this document. Personal information is defined as having any **one** (or more) of the following contained within it: name, date of birth, medical information, contact information, financial information, or any other information that can identify the individual(s). Anonymised data is not classed as personal information (e.g. as the result of anonymous surveys). Sensitive information includes, but is not limited to, medical information and financial information.

Your Accounts

You should be issued with a club email account in the format XXX@bromleydivingclub.com. These passwords can be revoked by the secretary / chairperson and such are not considered secure from the point of view of transferring personal information.

You should make sure you have access to your new mailbox.

You have access to a cloud account registered under the above email. Currently this is hosted on Google Drive. This service is secure (as long as a proper password has been set).

Log in to your Google Drive account and change the password to something memorable. You should turn on 2-step authentication. Please note this should be removed when you leave your current post. Do not tell your password to anyone.

The secretary & chairperson have access to the mailbox server. If need be, they can reset your cloud password revoking access

(Chairperson & secretary only) - ensure you have access to the website hosting back-end and are familiar with how to reset passwords on members' email accounts.

(Secretary only) - set a reminder on your calendar a few days before the indicated expiry of mailbox passwords. You should reset and re-issue passwords every 6 months to committee members. This does not affect the Google Account passwords.

Storing & Accessing Cloud Data

All cloud data is stored on Google Drive. You should work through an online interface and not store local copies of personal data. If you need to save personal data locally, this should be deleted as soon as you are finished with it. Wherever possible, keep your work in the cloud.

Once you leave your post, and a handover has been completed, you should disconnect your devices from the cloud account and delete any local copies that could remain as a result.

In your Google Drive account is a shared folder named "Committee Shared Files". These files are accessible by the entire committee. You should only store documents here, for which there is a legitimate need for all committee members to have access to. These include:

- Committee Meeting / AGM / SGM minutes
- A basic membership list (names, email, telephone, diving qualifications)
- Any document that contains no personal information
- Club financial records (with personal financial information removed)

Documents that should **not** be stored in the shared folder include:

- Personal medical information
- Personal financial information
- Other documents where the whole committee does not have a justifiable need to access the data in the normal operation of the club.

Sensitive information (e.g. financial, medical) etc. should be stored in your Google Drive but **not** in the committee shared folder. You may share the files with committee members who need access to the information (e.g. the treasurer for financial information, or the DO for fitness to dive purposes). If you are unsure, ask the data controller.

Sharing Data & Information Between Data Processors

Committee business should only be conducted from your club email address. If you receive an email to your personal email, forward it to your club email before responding, so an email trail is present.

Personal data (other than names) should not be sent via club email. To transfer sensitive information or personal data between data processors, you should share the individual file (or folder containing relevant documents) with the committee member(s) with whom the information needs to be shared with. You may send an email referencing that a folder has been shared, but it should not contain any personal data (other than names) in itself. You can share a folder from within Google Drive.

You should only share data with committee members who have a legitimate need to see all of the information in the document(s). If this is not the case, you should consider not sharing the document(s) or redacting any irrelevant information.

Communicating within the Club & Making Members Aware

During your role, you may need to communicate with the club as a whole. Please bear in mind the following:

- Personal information (except for names only) should not be distributed to club members without the written consent those whose data you wish to distribute.
- If emailing members, you should not include their names in the “to” column. You should either place all email addresses in the “BCC” column. You may used a mailing list system that has been approved by the committee. Note that club email addresses (ending in @bromleydivingclub.com) are non-personal information as they need to be publicly available to club members.

Personal data may be shared with a dive marshall for a dive trip. This data should not be retained by the marshall, and the issuing data processor should take appropriate steps to ensure this.

All members should acknowledge and agree to the privacy statement if we are to retain any personal data on them. They may also provide written restrictions on the use of their personal data.

Membership secretary only - maintain a data protection register, summarising members' wishes concerning their personal data.

Everyone should check the register on regular occasions, especially when dealing with the information of a new member. These wishes are paramount to the club's interests and may only disregarded if there is a legal requirement to do so.

Sharing Data Outside the Club

We routinely share data with BSAC as part of the management of the club. This will be done in accordance with their data sharing agreement, which you can find a copy of in the shared committee documents or on the BSAC website.

If you are not sure which data should be shared with BSAC, consult the data controller.

You may need to share data to another organisation. With few exceptions, the member(s), whose data is to be shared, should be asked for their consent. Data should not be shared without member's consent (except if we are legally required to do so or if obtaining their consent may lead to their or others' harm). If you are unsure, ask the data controller.

What to do if there is a Data Breach

If you know of a data breach, or suspect one has occured, you should report it at the first instance to the data controller. They will then lead an investigation to the nature of the breach and ensure that the proliferation of personal data is minimised. This will follow with a review of how the breach occurred and remedial action taken.

All data processors are expected to give their full cooperation to the data controller in the event of a data breach.