DATA & PRIVACY

CURRENT POLICY ESTABLISHED JANUARY 8TH 2018
LAST REVISED AUGUST 8TH 2024

When joining Starfleet Command Quadrant 2 (SFCQ2), you provide information about yourself when you register for membership through our Enlistment form online, or by paper membership applications at an event. This is considered personal data. We collect and store this information to fulfil club responsibilities and fulfilment of our membership services.

Where we need to collect personal data to fulfil club responsibilities and you do not provide that data, we may not be able honour or administer your membership or entry into SFCQ2.

Starfleet Command Quadrant 2 is committed to safeguarding your privacy and personal information you share with us as part of your membership. This privacy policy applies to both our collective website and membership services and is strictly applied from our main core of SFCHQ (administrative staff) through to Unit's on the ground.

If you have any questions about our Data & Privacy Policy or our treatment of the information you provide us, please write to us by email at **info@starfleet-command.co.uk** or use our contact form to speak to our Director of Communications directly.

The following outlines the data we collect and how we manage the information.

FURTHER DISCLOSURES

In addition to the disclosures reasonably necessary for the purposes identified elsewhere in this privacy policy, we may disclose information about you:

Personal data submitted by members is utilised at the discretion of the Director of Fleet Administration (Admin). As the controller of all submitted personal data, Admin is responsible for what data is collected, how we use it as a club and how that data is managed.

SFCQ2 is a community centric organisation where members join to interact with others. However their membership forms a contract between our data controller (Admin) and themselves (Member) for the term of their membership. As such, their personal information submitted as part of their membership must be treated appropriately and securely at all times.

Commanding Officers act as Processors. They may not make changes to how and why we collect data, however they may use it as needed to perform their duties off leading their individual units.

As a processor, Commanding Officers must follow the guidelines set out and are only allowed to act on the strict instructions set out below.

BASIC INSTRUCTION

As a Processor, a Commanding Officer upon receipt of their acknowledgement of responsibility is granted the ability to utilise information they have access to strictly for the purpose of membership management within their specified Unit within Quadrant 2.

Commanding Officers are granted direct access to the SFCQ2 database for the purpose of club

operations. A CO may use the information for club related tasks, invitations, event planning and communications with each member.

This data is split into three categories. Personal Data, Fleet Data and Member Notes.

1. **Personal Data**
   Personal and identifying data includes anything that can cause risk to a member of SFC is exposed. This includes the members name, date of birth, home address and email address.
   1. Access to personal data is strictly for fleet use only. Commanding Officers must only utilise this data in handling any club related matters, such as sending certificates and awards through email or post; communication between CO & Member and group invitations.
   2. Commanding Officers must not share the personal data of any member to any other member. This includes exposure to contact information including passing along phone numbers, addresses or failing to Blind Carbon Copy in mass emails.
   3. Members can volunteer for their information to be passed to another for the purpose of club operations – such as organising a group chat via phone apps or in event planning, however a Commanding Officer must have written permission of that member to disclose such information and a record kept of any such action.
      1. Commanding Officers should take extra care in this regard if setting up a chat group via a third party app, ensuring all members sign off on being added to such groups if their personal data such as email address or phone number is exposed.
      2. Mass emails to crew should also be sent via "Blind Carbon Copy" without the entire units email exposed in a "To" or "Carbon Copy" line.
   4. Personal data cannot be altered by a Commanding Officer. If any member wishes to update their information, such as a change of address, they must be advised to inform the controller either through the appropriate function within our Membership Hub or by direct contact via email.

2. **Fleet Data.**
   While commanding officers are restricted from making changes to a members personal data, a CO can altered a limited amount what we refer to as fleet data. Fleet Data is simply membership tiers and rewards in line with the SFCQ2 core guidelines.

   These Tables include;
   A Rank (in constraints with the Officers Handbook)
   A Department
   A Assignment (or Role)

   CO's can change these tables based on their own decision making in line with their responsibilities and commitments in the role as normal. However, any changes should be reported at the earliest opportunity to Admin.

   All other Fleet Data should not be altered by anyone other than the Administrator.

3. Unit Transfers
   Unit placements are labelled in the database as "Post". Unit transfers can be at the request of a member or on occasion, administrative measures. Transfers can only be actioned by Admin and follow a strict process.

   At no point should a Commanding Officer transfer or action a transfer for any member of SFCQ2. If an officer asks a CO to action such a transfer, they should be referred to the correct procedures either through the appropriate function within our Membership Hub or by direct contact via email to Admin to ensure all parties are aware and follow Admin procedures.

INFORMATION HANDLING (better header please)

....

1. Disclosure & Sharing of Information.
   All Commanding Officers with access to the Fleet Database are responsible for ensuring only they have access to the information within. This includes not disclosing personal data to;
   - A An Executive Officer or any appointed staff roles.
   - A Any other member of SFCQ2 in any unit.
   - A Any other CO or SFC Senior members, excluding discussions with Admin
   - A Any Outside parties.

   Any such sharing would be considered a breach of data protection policies, and an act of misconduct within SFCQ2.

2. Consent
   Due to the nature of SFC, some events or occasions may require sharing information. Ff for example in creating group chats or in organising events. In such a scenario, a CO can coordinate sharing of contact information between two parties if:
   - A Members involved consent to their information being used
   - A The information is being used in line with SFC requirements
   - A The CO takes great care to ensure the safety and protection of members.

   A CO cannot share any personal or identifiable data of any member without their direct consent. In such scenario's written direct consent must be appropriated by the member. This can include informal written consent, such as in text or via a messengering service, however this must be documented by the CO.

3. Data Retention Length
   SFCQ2 only holds data for active members. We only retain a members information for the length of their time with us. When a new member joins within a CO's region, the CO will be informed and the database updated.

   If any member, for whatever reason, chooses to leave or close their membership, upon receipt of the information upon confirmation from Admin, a CO must remove any and all records from their files and erase the persons details from all records.

   Admin will remove a persons data within fourteen days of confirmation or direct request of their account deactivation and a copy off our data policy. Under no circumstances should any outgoing person be contacted on behalf off SFC.

4. Sub Processors
   As the person responsible for the data they are processing, a CO must not under any circumstances delegate the task of data management to any other party (a sub processor) such as a senior member of staff, executive officer or any outside party.

   If at any point a CO is unable to perform their duties, for example due to an extended leave of absence, information handling will fall back to Admin; Executive Officers should coordinate with Admin to ensure any communication requirements.

5. Executive Officers
   Part of an Executive Officers (XO) role in any unit is to take on the responsibility of leadership if the CO stands down or is dismissed. As part of their role, all Executive Officers should be briefed and aware of their role with an understanding of our data handling policies and instructions from Admin.

   All CO's should make all documentation available to their XO. If a unit is passed over due to a

CO standing down from the role, their XO should be briefed and ready to agree to all relevant documentation.

As with a Commanding Officer, An XO will not be granted full permission to act as a processor or have access to any data until completion of documentation.

6. Access Rights
A CO will be granted access upon all outlined terms. Once a CO steps down or is dismissed, they no longer have the right to access or retain personal information. All accessibility for the former CO – inclusive of database and email access - will be revoked immediately and the CO must, without hesitation, delete all files, information or logs held on file and not retain, misuse or abuse any personal information.

Once a term of a CO is over, for whatever reason, that CO no longer has rights or need to access this information.

NOTIFICATION OF BREACH
In the event of an data breach, regardless of severity, Admin must be informed without undue delay by no other communication than directly to Admin's email detailing;

A The nature of the data breach
A The date and time off the breach.
A Which member, or members, have been effected.
A How the breach occurred.

This can be completed via direct written contact via internal SFCQ2 email, or by completing our incident report form template.

Once a breach has been reported to Admin/SFCQ2, it will then be assessed through the Information Commissioners Office (ICO) to assess severity and action. This may result in a self report is severity is high enough. Though regardless of their assessment, SFCQ2 Admin will retain and file a incident report.

DISCLAIMER
Data subjects (members) can bring claims directly against processors (CO's). A processor is liable for the damage caused by its processing activities only where it has not complied with legal obligations under GDPR or followed the instructions set out herein.

While SFC is liable for major breaches, CO's must not deviate from instruction as if they are responsible r fail to act in accordance with out instruction, they could face liability themselves.

As such a Commanding Officer must understand and abide by these instructions with no deviation.