# Data Protection Policy

## Context and overview

## Key details

| | | |
|---|---|---|
| Policy prepared by: | Robert Hall | |
| Approved by council on: | 31/03/2018 | |
| Policy became operational on: | 25/05/2018 | |
| Next review date: | 31/05/2018 | Council 116 |

## Introduction

To effectively discharge its business duties the Challenger Society for Marine Science (hereafter referred to as "The Challenger Society") is frequently required to gather and retain information relating to both individuals and groups, including Society members, academic partners, business associates and others with whom the Society needs to develop a relationship or otherwise interact. The purpose of this data protection policy is to clearly set out the procedures by which personal data must be collected, handled and stored to meet the Society's data protection standards and to comply with the law.

## Why this policy exists

This data protection policy ensures that the Challenger Society:

- Complies with data protection law and follows good practice
- Protects the rights of Society members, employees and business contacts
- Is open about how it stores and processes individuals' data
- Protects itself from the risks associated with a potential data breach

## Data protection law

The General Data Protection Regulation 2018 applies to all companies and organisations, anywhere in the world, which process any information about EU citizens. It is global in reach and includes a broad definition of the meaning of 'personal information'. It describes how organizations such as The Challenger Society must collect, handle, and store personal information. These rules apply regardless of whether data are stored electronically, as hard copy or on any other medium. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The General Data Protection Regulation 2018 is underpinned by eight important principles. These state that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary

6. Be processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless the destination country or territory ensures an adequate level of protection

# People, risks and responsibilities

## Policy scope

This policy applies to all Challenger Society council members, ordinary members, volunteers, contractors and other individuals working or volunteering on behalf of the Challenger Society.

It applies to all data held by the Challenger Society that relates to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation 2018. Such data may include:

- Names of individuals
- Postal addresses of individuals
- Email addresses of individuals
- Telephone numbers of individuals
- Any other information relating to individuals

## Data protection risks

This policy is designed to protect the Challenger Society from tangible security risks, including:

- **Breaches of confidentiality;** such as the inappropriate distribution of personal information.
- **Failure to offer choice**; for example, contravening the right of an individual to freely choose how the Challenger Society uses data relating to them.
- **Reputational damage;** as may occur for example if any data held by The Challenger Society is unlawfully accessed by unauthorised persons.

## Responsibilities

Everyone who is involved with the business of the Challenger Society has a responsibility to ensure that data collection, their subsequent handling and storage are all carried out appropriately. Anyone who handles personal data must ensure that they comply fully with this policy and its data protection principles.
Selected Challenger Society members have the following key areas of responsibility:

1. Officers and Council members are responsible for ensuring full compliance with the requirements of the General Data Protection Regulation 2018, thereby guaranteeing that the Challenger Society meets its legal obligations.
2. Those Challenger Society members who lead Special Interest Groups on behalf of the Challenger Society have responsibility for protecting data held (contacts or other sensitive personal data) at all times.
3. The Data Protection Officer is responsible for:
    - Keeping Council updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, according to a pre-agreed schedule.
    - Providing data protection advice to all individuals covered by this policy.

- Addressing data protection questions arising from any individual covered by this policy.
- Dealing with requests from individuals to access data held about them by the Challenger Society (subject access requests).
- Checking and approving any contracts with third parties that may require access to any data held by the Challenger Society.

## General guidelines

- Full access to personal data held digitally by the Challenger Society is restricted to the following four Council members: President; Honorary Secretary; Honorary Treasurer; Membership Officer[1].
- Data should not be shared informally.
- Access to data covered by this policy is restricted to persons requiring them for the effective discharge of duties associated with Challenger Society business.
- Data security must be ensured by taking the appropriate precautions, including the use and regular updating of strong passwords.
- Personal data should not be disclosed to unauthorised persons, whether they be Challenger Society members or external parties.
- Membership data will be fully audited during quarterly council meetings of the Challenger Society, where reviews of data retained will be carried out. Data pertaining to members who have failed to renew their annual subscriptions will be deleted from the Challenger Society data records a maximum of three months following membership expiry.
- The Membership Officer will act as Data Protection Officer for the Challenger Society and will advise Council members and address individual member requests in respect of any aspect of data protection.
- An unauthorised person is defined as anyone who is not currently a member of the Council of the Challenger Society, or is not specifically appointed as a contractor by the Council.

### Data storage

These rules describe how and where data should safely be stored.

In general, the Challenger Society operates a digital data holding policy. Member personal details (email addresses, general preferences, etc.) are maintained digitally on a secure server provided by an approved web-hosting contractor. The servers provided, use 128 bit encryption, with access restricted to those officers identified in the General Guidelines.

If data are stored **as hard copy**, they should be stored securely to preclude unauthorized access. These guidelines apply to data routinely stored electronically but which may periodically be printed for specific purposes:

- When not required, hard copy data should be kept in a **locked** draw or filing cabinet.
- Hard copy data should not be left where unauthorized access is possible, such as on a printer or on an unattended desk.
- Data printouts should be **shredded** and disposed of securely when no longer required.

Data that are stored **electronically** must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

[1] See Appendix 2

- Data should be protected by **strong passwords** that are changed regularly and never shared.
- Any data stored on **removable media** must be **locked** away securely when not being used.
- Data must be stored on designated secure (encrypted) servers only.
- Data must be held only on an approved cloud computing system (Dropbox) with access designated to specific Challenger Society Council Members when authorised by one of the officers listed in Appendix 2.
- All membership data must be **backed up** monthly by the membership officer.
- Where data are transferred to laptops or other mobile devices (e.g. tablets and smart phones) for reasons of transit, their management and protection will enjoy the same level of security in respect of passwords and access until such time as the data are destroyed.
- All servers holding Challenger Society data must be protected by approved security software and a firewall.

## Data use

Personal data are at the greatest risk of loss, corruption or theft when accessed for subsequent use:

- Personal data should not be shared informally. Personal information will not be sent in the contents of email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.

## Data accuracy

The law requires that the Challenger Society takes reasonable steps to ensure data are accurate and up to date. The greater is the need for personal data accuracy, the greater the effort the Challenger Society will direct towards ensuring this. All Challenger Society members have a responsibility to ensure that their personal data are as accurate and up to date as possible. Members of the Council of the Challenger Society are responsible for ensuring the means by which members can maintain their data up to date. This will be facilitated via secure access to the Challenger Society website and portal.

## Subject access requests

All individuals whose personal data are held by the Challenger Society are entitled to:

- Request what information the Society holds about them and why.
- Request and be granted access to it.
- Be informed about how to maintain their details up to date.
- Be informed about how the Challenger Society meets its data protection obligations.

If an individual contacts the Challenger Society requesting information, this is referred to as a subject access request. Subject access requests should be made via email (members@challenger-society.org.uk or contact@challenger-society.org.uk). The Challenger Society undertakes to fulfil such requests within one month of receipt and to verify the identities of all individuals making such subject assess requests prior to releasing any information.

## Disclosing data for other reasons

Under certain circumstances, the Data Protection Act allows the disclosure of personal data to law enforcement agencies without the consent of the data subject. In these instances, the Challenger Society will disclose the requested data, having first ensured that such requests are legitimate and after seeking legal advice as necessary.

## Providing information

The Challenger Society aims to ensure that individuals are aware that their data are being processed, and that they understand:

- How their data are being used and for what purpose
- How to exercise their individual rights in respect of these data

To these ends, the Challenger Society has a privacy statement that defines how data relating to individuals are used. This is available on request, or it can be accessed through the Challenger Society website (www.challenger-society.org.uk).

# Appendix 1

## Membership Data Audit

Members personal data held digitally by the Challenger Society for Marine Science

Data provided by the member:

Title
First name
Surname
Primary email
Secondary email
Institution
Address 1
Address 2
Address 3
Post Town
Postcode
Membership Type
Option to Receive emails
Option to receive Hard Copy of Ocean Challenge
Option to grant Gift Aid
Option to join Special Interest Group

Further data created and held digitally by the Society:

Membership ID
Method of subscription payment
Date subscription paid
Date of Expiry
Ordinary Membership or Fellow

# Appendix 2

## Current officers of the Council of the Society (10/04/2018)

| | |
|---|---|
| President | Rachel Mills |
| President Elect | Robert Upstill-Goddard |
| Honorary Secretary | John Bacon |
| Honorary Treasurer | Edward Mawji |
| Membership Officer | Rob Hall |