Document Control Information

NB: If you are reading this as a printed document you are requested to check the Controlled Documents Master List to ensure that it is the latest version before following the guidance it contains. If you discover this version is out of date, please destroy it and use the latest version.

Document Details	
Document Name	Member Groups Good Practice Guide for Data Protection
Purpose of Document	Governs the sharing of Member Data with Member Groups in line with Data Protection Laws and Regulations
Document Number	Pol 122
Document Version Number	V1.1
Document Status	Approved
Document Owner	Head of Community
Data Classification	Public – External
Security Category	Low
Prepared by	Rachael Levermore
Date of First Draft	February 2020
Date Approved	October 2020
Approved by	Head of Compliance
Next Scheduled Review Date	**November 2022**

Version History			
Version Number	**Date Amended**	**Changes Made**	**Checked by**
V1.1	24/11/2021	No changes	J Jeffrey
V1.0	01/10/2020	Removed references to membership assessors	J Jeffrey

Distribution List	
Name	**Title**
	All Staff
	All Members via Volunteer Portal
	Policy Committee

Making IT
good for society

BCS, The Chartered Institute for IT

Member Groups Good Practice for Data Protection

October 2020

CONTENTS

This document forms part of our Management Systems and compliance is mandatory for all staff and contractors. If you find any weaknesses in the document or examples of non-compliance, please report it to the Compliance Team at infosec@bcs.uk .

Introduction

These guidelines has been designed to ensure that BCS volunteers are aware of their responsibilities when it comes to processing data as there are significant implications in terms of fines (to BCS and volunteers) as well as reputational damage if we do not do this correctly.

Under data protection law, all organisations and individuals processing data have an obligation to ensure that operational measures are taken to ensure the security, safety and privacy of the personal information we process.

BCS members are able to join one or multiple Groups and Branches committees by being co-opted onto a committee or through an election at an AGM.

BCS is the data controller for member and non-member data processed within the BCS Group and it has a responsibility to its members to maintain the safety and security of their Personal Data.

1. Access to Data

Members' data is not made available or accessible directly to volunteers within the Member Groups community as we do not have their consent to share this information.

We recognise that Chairs of the various Groups and Branches require certain information and are able to request Business Intelligence reports covering a wide range of useful information such as member joining/leaving numbers, age ranges and location data by contacting their community co-ordinator.

This information will be provided in an anonymised format which contains no personal data about members but will provide key information needed for matters such as preparing for and running annual general meetings and the planning and co-ordination of events.

Requests for reports are typically processed within five working days.

2. Member Group Communications

It is key that Member Groups can contact their constituent members and inform members about events and news relating to the group.

All electronic message broadcasting will be carried out via the list servers provided. Nominated committee members, who hold professional membership grade or above of BCS, have the permission levels to post to these lists directly.

The data in our membership database, including non-member lists will be processed and managed by the Member Groups team.

Please note that Committee Members can choose to hold the contact details of their fellow committee members in much the same way you have the contact details for colleagues at your place of employment. In these circumstances, BCS does not hold any responsibility for the

data that Committee Members hold but you should obtain consent from the person(s) whose details you wish to keep. For the avoidance of doubt, BCS holds no legal responsibility for the processing and handling of this data.

All communications for marketing events, newsletters, callouts for AGMs, additional benefits, or general group updates must be done via the list servers or via your community co-ordinator.

3. Pre-Registered Events

BCS uses the ticketing platform, Eventbrite for the purposes of managing the booking of its events.

The community co-ordinator will set up a new event on Eventbrite for all member groups. To ask for a new event to be created please complete the Event Booking Request Form which can be downloaded here and return it to groups@bcs.uk.

Members will then register directly with Eventbrite to book a place and this information is returned to BCS.

All events which attendees must pre-register to attend must be created and managed by your Community Coordinator on the designated platform.

4. Open Events

All attendees who go to events that have open attendance (i.e. “on-the-day sign-in”) are required to complete the sign in sheet when they arrive.

These sheets must be managed by the Chairman or a nominated deputy who must have sight of the sign in sheet at all times. This is to protect the contact details of the individuals who have registered. Once completed, this sheet must be returned to the community co-ordinator within 3 days of the event using either password protection or encryption. The password for files must be sent in a separate email to the file itself in line with standard information security process. The hardcopy of the sheet must be destroyed securely after confirmation of receipt from the community co-ordinator. The co-ordinator will then enter the contact details of all non-members who have agreed to receive future communications in the list server.

5. Non-Member Registration

We encourage non-members to attend our events to get an understanding of what we do before they commit to becoming a BCS member. Non-members are also able to subscribe to BCS communications by asking to join our mailing list. The collection of non-member data will be held and processed centrally by BCS.

The community co-ordinator can set up a new email distribution list if your group does not have one.

6. Unsubscribe

BCS members can unsubscribe or update their marketing preferences by logging on to MyBCS. Non-members who no longer wish to receive marketing communications from BCS should either reply to the email with ”Unsubscribe” in the header or contact **custsupport@bcs.uk** asking that their name is removed from the mailing list.

7. Notification of a Breach

If you have reason to believe that you have caused a data breach, such as emailing personally identifiable information to the incorrect recipient you must notify BCS immediately by sending an email to us at breach.notification@bcs.uk.

Groups who operate outside of these guidelines will be subject to the disciplinary processes set out in the Member Group Rules available on the Volunteer Portal.

8. Policy Review

This policy is reviewed on an annual basis in line with departmental quality standards and regulatory criteria. We will also consider any customer feedback, trends from our internal monitoring arrangements, changes in our practices, as well as changes in legislation. If you would like to feed back any views, please discuss with the owner of this document.

BCS, 3 Newbridge Square, Swindon, SN1 1BY
T +44 (0) 1793 417 655
Email **groups@bcs.uk**
Website **www.bcs.org**