GENERAL DATA PROTECTION REGULATIONS 2018
AND
MILFORD ON SEA HISTORICAL RECORD SOCIETY

As our Society collects and stores personal data on members, which means information that can identify them, we need to comply with the new General Data Protection Regulations (commonly known as GDPR) which comes into force on May 25th 2018, replacing the current Data Protection Act.

I have looked into the requirements of the GDPR as they affect clubs and societies, because, in order to operate the Society, we need to store the details of our members.
GDPR may seem onerous and heavy-handed for societies like ours, but it is designed to help put a stop to unscrupulous organisations selling on customers' details to others so we all then get plagued with Junk Mail, Spam and telephone calls asking us about an accident we've never had or debts we don't have.
It is very simple for MOSHRS. Even if we feel it is unnecessary there is a legal obligation to demonstrate compliance with the data protection principles, the absolute basic requirement being a lawful reason to collect personal data and the Charity Commissioners insist on this.

THE LAW
You can collect and process personal data if:

- You have the consent of the data subject.
- It is in the legitimate interests of the data controller (e.g. membership secretary).
- It is necessary for the performance of the contract with the data subject (i.e. you need to send members details of meetings, events etc as part of their membership).

So – what do we need to do to comply with the GDPR after May 25th?

We do NOT have to register with the Information Commissioner's Office, although we could if we wanted to. Whether registered or not, this is the body to whom people can complain if they think we are mishandling their personal details, at which point we may need to demonstrate how and why we store and process personal data.

PERSONAL DATA is defined as:
"Any information relating to an identified or identifiable natural person (referred to as the Data Subject). A person is identifiable if they "*can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors, specifically the physical, physiological, genetic, mental, economic, cultural or social identity of that actual person*".

Information gathered on membership application forms, such as names, addresses, telephone numbers and email addresses is all personal data. So too is the information collected about visitors and potential members, and it can include references to people in emails.
This data can only be processed lawfully, fairly and transparently.

PROCESSING is defined as:
"Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, determination or otherwise making available, alignment or combination, restriction, erasure or destruction".

So as we need to keep a list of society members and their contact details (whether in a book or on a Computer) it is processing, we must assume that any use we make, or wish to make, of the personal data, as well as collection, storage and destruction of it, will be governed by the GDPR.
As we already (loosely) comply with the current Data Protection Act, we are well on the way to complying with the GDPR, but we had to establish if our current policies and procedures are suitable to

comply with the GDPR and, if they are not, alter them. This was carried out by a review of what we do currently.

THE REVIEW

I considered:
What personal data we hold.
Whether we really need it.
Where it came from and the basis on which it was collected.
What we do with it and what we are planning to do with it.
Where and how we store it.

AND WE SHOULD DOCUMENT THIS – HENCE THIS PAPER

We obtained the consent of each individual when we collected their data, after all they filled in an application form for membership of their own free will and handed it to us.
We will have told them at the time what we would use this information for.(eg to send information to them about our programme and events). The Regulations make it clear that it is very important that the data is only used for the purposes that were made clear at the time it was collected. If we do not have consent to use the data for any purposes you subsequently intend to use it for then it has to be collected again with the appropriate consent request.
Any consent needs to be explicit so it must be an "opt in" by ticking a box or providing a signature indicating they have read why this data is being collected, what it will be used for. Wee comply with this fully at present. The only bits we do not currently do is include information on how it will be stored, and the fact that they can have it removed on request within 30 working days of such a request.

SOCIETY DATA PROTECTION POLICY

The strict obligations on maintaining records specified in the GDPR are unlikely to apply to MOSHRS but a prudent approach would be to formulate a society data protection policy which records:
• The purposes of the processing.
• The categories of data subject (members/honorary members etc) and categories of personal data relating to them (names, addresses, telephone numbers, email addresses, date of joining etc).
• The recipients/categories of recipients of the data (society officers).
• A general indication of time limits for erasure – for example of members who do not renew – and how it will be destroyed.
• A description of any security you use.
This information needs to be identified in any case to decide what steps we need to take (if any) to comply with the GDPR.
Whilst it's not essential, it might be a good idea to give the role of data protection officer to Membership Secretary to ensure the policy and procedures are adhered to.

IN A NUTSHELL

I recommend that on our membership application/renewal forms should include the following wording printed as 'small print' but large enough to be read and that we should operate in accordance with this at all times:

'The information you have provided on this form will be used by the society for purposes only in connection with the running of the society, which includes communicating by post, telephone and email. It will never be disclosed to third parties or used for marketing purposes.
The data is stored on a computer and backups are kept on external disk drives. The data may be provided to committee members and other members by email or telephone when it is needed to facilitate the running of the Society and provide the benefits of membership to you.
Your details can be removed from our stored records within 30 working days of a written request to the membership secretary.
You have a right to complain to the ICO if you believe there is a problem with the Society's handling of your data.
Please sign below to indicate that you have read and accept these terms.'

PRACTICALITIES

We should…

Only collect the information really needed and be clear on the application form what it will be used it for.

Store application forms securely and consider who needs to see them and how long they will be kept (bearing in mind you may need to be able to show they consented before they next renew).

Make sure membership information is kept up to date. Ask members to check their information at renewal and provide an easy way for them to update it. Destroy their previous forms 6 months after the end of the Membership Year (ie on 1st July for the previous year).

Destroy information about former members in line with the above time period.

The identity and contact details of the membership secretary must be included on the form.

For more detailed information about the GDPR as it affects organisations, visit
https://ico.org.uk/for-organisations