General Data Protection Regulation Awareness Document

What is this all about?

New legislation called the General Data Protection Regulation (GDPR) comes into force on 25th May 2018. It is European legislation that will be adopted into UK law after Brexit. This will replace the 1998 Data Protection Act and it is being overseen by the Information Commissioner's Office (ICO).

It is specifically targeting 'sensitive data'. This is data that, either on its own or combined, will enable a 3rd party to be identified.

Why is it important?

1. This forces entities to put greater emphasis on the protection of the data supplied by members, staff and others from which data is gathered.
2. In this increasingly hostile IT environment, there is a need to protect business data from hackers intent on using this for gain, including the recently publicised ransomware attacks.
3. Noncompliance will cost dearly. The ICO has the power to impose fines of the greater of approx. £8,000,000 or 2 percent of turnover.
4. A breach of data could damage the reputation of the organisation
5. The resulting cost of clean up after the breach could be huge
6. You should ensure that culturally, data safety is considered in every aspect of the entity

What does compliance look like?

To prove that you have the consent of the 3rd party:

- You must be able to prove that 3rd party consent was given
- The written consent obtained must be clear, intelligible and easily accessible
- As consent can be withdrawn at any time, you must make it easy for the 3rd party to do this and you must be able to delete all data that you have in relation to that person
- Processing the following types of personal data are prohibited unless documented consent is given (there are exceptional circumstances where this can be collected, contact the Information Commissioner's Office where this becomes an issue)
    - Race
    - Ethnic origin
    - Political opinions
    - Religion
    - Philosophical beliefs
    - Trade union membership
    - Biometric data
    - Health data
- You must be able to provide documentary evidence that your systems are secure
- You must have a reporting procedure that would be activated in the event of a breach

What do you need to do about it?

1. Appointed a Data Protection Officer

2. Along with this awareness document, you should meet with your team to thoroughly examine the systems used and the security surrounding your data. This may involve changes in processes and extra layers of security.

3. Where you use data to communicate with members etc. you will need to contact them to get documented permission to continue to send them information and use their data.

4. Your IT framework should be kept secure by:
    - Installing the latest updates
    - Having firewall protection
    - Maintaining a high level of email protection
    - Ensuring that your website is secure
    - Work with 3rd party system providers to evidence their compliance with GDPR
    - Identifying and resolving security vulnerabilities caused by the continued use of old software, systems and hardware
    - Encrypting data where appropriate
    - Ensuring daily backups are taken and off site backups are maintained securely to guarantee business continuity in the event of a breach
    - Fully document the IT infrastructure (software and hardware) to enable a faster resolution in the event of a breach of security

5. Mitigate a suspected attack or breach by:
    - Appointing a person to notify
    - Having documented procedures of what to do in the event of a breach

6. Establish procedures following a breach
    - Notify the Data Protection Officer
    - Inform the ICO of the breach within 72 hours of the suspected breach where applicable
    - Resolve the breach
    - Work with ICO on the breach investigation (if applicable)

<u>What can your team do to help?</u>

Here are some of the areas in which your team can assist in this process:

- Read all communications concerning GDPR and attend the training given
- Ensure that your Data Protection Officer is aware of any 3rd party software used in performing club duties
- Ensure that sensitive documents are password protected
- Ensure that strong passwords are used (upper case, lower case, numbers and symbols)
- Periodically change passwords (monthly or quarterly)
- Do not open suspicious emails, especially those with attachments, especially '.exe' files
- Special conditions apply to data from those under the age of 16. Where this is encountered, please contact the ICO as additional compliance checks are required
- Report any suspected data breach to your Data Protection Officer