



Data Protection

Social Media and

Internet Policy

**Introduction**

Pelicans Hockey Club understands that the internet as well as mobile communication and Social Media are a valuable and increasingly used form of communication both at home and for Pelicans Hockey Club business and social activities.

This Policy relates specifically to the use of the internet and social media by Pelicans Hockey Club members and affiliates. ‘Social Media’ as referred to in this policy means media such as blogs, web forums, all social networking sites including but not exclusively Twitter, Facebook, YouTube and Linked In, instant messaging and other publicly available communication and content-sharing systems and sites.

This policy does not seek to regulate use of social media by Pelicans Hockey club members or affiliates in a purely private capacity **provided** this does not have or could have a negative impact on Pelicans Hockey Club or its members, affiliates or associations. It further intends to protect Junior or vulnerable members.

What it is intended to do is to ensure that you understand the rules governing internet and social media use in particular when making reference to the club or it members or affiliates. The ultimate aim is to maintain consistent standards.

In particular, this policy requires you to;

* Abide by this policy and all other relevant policies whenever their use of social media relates to Pelicans Hockey Club and its affiliates whether the intended use is personal or professional
* Act in a professional and responsible manner and exercise common sense, particularly bearing in mind any negative impact their social activities might have on the reputation of the club
* Understand that when posting messages using social media they are making public statements. As such those messages will not be private and can be forwarded by third parties without their consent.
* Consider the potential sensitivity of disclosing information (such as health) to the world. Once sensitive information has been disclosed, it cannot be recovered and this may result in liability for both the club and individuals.

**Scope**

This policy applies to ALL members, junior and adult, associated members and affiliates or representatives of the club or players.

Each of which is expected to familiarize themselves with this policy and comply with its terms.

Any new or amended policies will be made available to all members.ction

**Data Protection Policy**

Pelicans Hockey Club has adopted England Hockey (EH) Data Protection Policy which endorses fully the statements and the intent of the Data Protection Act 1998. The Data Protection principles contained in the Act are designed to protect the rights of the individual. England Hockey is registered to hold data under the Data Protection Act.

**Definitions**

Personal Data means data (manual or computer) which relate to a living individual who can be identified from those data (or from data and other information that is in the possession of, or is likely to come into the possession of, the data controller).

Data means information that is being processed automatically or is recorded with the intention that it should be processed automatically. Any manual data that forms part of an “accessible record” is also included in this definition.

Data Controller means a person who determines the way in which any personal data are to be processed.

**Notification**

Any time that data about an individual person is held manually or on a computer, the purposes must be:

o In accordance with the principles of the Act o Available to be seen by the person named o Notified to the EH CRM and Membership Officer

**Processing**

Every person must be sure that data held on manual and computer files about individuals is:

o Processed fairly and lawfully o Accurate and up-to-date o Used only for defined purposes o Kept private o Kept only for as long as it is useful o Relevant and not excessive ND HOCKEY POLICY DOCUMENT – DATA PROTECTION

**Disclosure**

Care should be taken to ensure that the identity of any person requesting information about themselves is confirmed.

Any time that information from a file is given to a third party, the person giving the information must be sure that the third party is properly identified, and authorised and registered to receive the data

Before disclosing personal information to a third party it is essential to check why the data is required and to whom that party intends to disclose it. Only disclose personal information when you have checked that the disclosure is compatible with your disclosure policy and the Data Protection principles.

If you are aware of any data held or disclosures made that break the data protection principles you must report this to your line manager, or to the CRM and Membership Officer, in order that the breach may be addressed.

**Policy on Authority to Access**

The Computer Misuse Act 1990 identifies the legal framework for definition of and prosecution for unauthorised use or misuse of computers and computer systems. Whilst the Act is particularly intended to deal with unauthorised accesses from outside the organisation ("hackers"), it deals equally with unauthorised accesses from inside.

It is essential that you, as a computer user, understand the extent of your authority to use and access systems. Computers used for more than one purpose and those connected to the corporate data network provide the potential for access to a large number of systems and to a great deal of personal, private and confidential data.

This policy makes it your responsibility to guard and protect your ability to access systems that you have authority to use. Passwords must not be written down or passed on (other than to your line manager). Computers must not be left logged in when unattended, particularly those in open access offices.

Any employee or volunteer, finding that they have access to systems and data which they are not authorised to use must report this to their manager, or a director, in order that the access may be removed. Any employee with authority to access data that is no longer necessary to their work must ask for the access to be removed. Any employee who knows that unauthorised access is taking place must report this to their line manager or to a director in order that the access may be removed.

**Penalties under the Act fall into two main categories:**

o Unauthorised access - Anyone gaining access, or attempting to gain access to computer data they are not authorised to see, may face a fine of up to £2,000 or six months in prison, or both.

o Ulterior intent or unauthorised modification - Anyone accessing data with an ulterior motive, or modifying data without authorisation, may be sentenced to up to five years in prison or an unlimited fine, or both.

**Data Security Policy**

o Make sure your password is changed regularly o Do not leave your computer accessible when unattended (a password-protected screensaver

can be a simple solution) o Make sure you are authorised to use the systems you need o Remember to copy data regularly for security and back-up. o Store important files in your folder on our network file server if you have one – these are

backed up regularly. o Ensure important email files are stored in an archive folder. o Do not store personal information on a laptop, it should be kept on the England Hockey

Board’s Server.

Contact us:

For more information, please contact Ian Wilson.

**Social Media Policy**

**Use as a representative of the Club**

When authorised to act on behalf of the club to use social media, you should:

* Only interact as a representative on social media approved by the committee
* Read and comply with the terms of use of any social media platform
* Ensure so far as possible that you know who you are communicating with. In particular be aware of attempts to try and obtain passwords or user names or sensitive information that may compromise other players or members
* Ensure you act responsibly. Confidential information should not be shared without express permission. If in doubt, do not post and consult a committee member for advice.
* Ensure any content that you upload to any social media site does not infringe any intellectual property rights belonging to any third party.

**Use of social media in a private capacity**

* We trust and expect you to take a responsible approach to your use of social media
* When using social media in a personal capacity you should not directly or indirectly represent that you are doing so on behalf of the club. For example, an opinion must not be expressed in such a way that it could lead someone to reasonably think they are the opinions of the club.
* Do not provide recommendations or references for anyone else on social media in any way which suggests any endorsement or recommendation by the club. If you wish to do this you should first gain express permission from a committee member.
* If you notice any positive or negative treatment of any player or member on social media it is expected that you report this to an administrator or committee member.
* In the event that you receive criticism of the club or a member in your comments transmitted via social media, consider carefully what should be the appropriate response. It may be better not to respond at all to negative comments than to make any comments which may simply give the effect of making the situation worse.

**Monitoring of use**

Social media platforms endorsed by the club will be regularly monitored by its administrators. If however you are concerned any posts or content is in appropriate, it is expected this should be reported to an administrator or committee member.

If there are concerns that your use of social media is inappropriate or damaging to the club’s reputation and its members or affiliates then such usage will be monitored and appropriate action will be taken. This may be in the form of asking for the post to be removed and where necessary the user removed from the social media platform.