GDPR Guidance for Volunteers 

Version 2.0 (August 2018)

The General Data Protection Regulation (GDPR) is a new EU legal framework which came into force on 25 May 2018. Its purpose is to give individuals more control and protection of their personal data. It introduces new regulations for all organisations that process (collect, manage and use) personal data. As Reading Hockey Club processes data, and our volunteers process data on our behalf, we are legally required to comply with the GDPR.

The GDPR outlines the conditions under which data can be processed. These principles are similar to the 1988 Data Protection Act, but more specific. For example, people have to opt-into rather than opt-out of communications. This means there are additional requirements that we now need to follow when we collect, manage and use data. The new accountability principle means there is now greater responsibility on organisations to document how they process and manage personal data. As Reading Hockey Club process data on behalf of our members, officials and volunteers need to work together to follow GDPR guidelines to ensure personal data is managed appropriately. Failing to do this may result in Reading Hockey Club and individuals being fined.

# Personal data

The GDPR outlines how personal data can be used. Personal data means any information relating to a living person who can be directly or indirectly identified by that information.

## Personal data includes:

* Name (title, first name and surname)
* Postal address (full or partial eg. postcode)
* Email address
* Telephone number (home or mobile)
* Membership number
* Online identifiers (such as IP address)

## Special categories of personal data

The GDPR also governs the use of sensitive personal data, which is now described as special categories of personal data - and there are stricter controls regulating the collection and use of this information. Sensitive personal data includes ethnicity, race, political affiliation, religion, health, sexual orientation etc. Such data needs to have even more robust processes around its use.

# Data processing

The GDPR, like the Data Protection Act, is about how personal data can be processed. Data processing means:

* Collecting data
* Recording and holding data (electronically or in paper-based filing systems)
* Any activity that uses the personal data (such as organising, adapting, changing, retrieving, consulting, disclosing, erasing or destroying the data).

Examples of data processing in the club are:

* Using the membership lists to send out match information
* Taking registration of attendees at a training session
* Filling in an Accident form
* Publishing information which includes members’ names and contact details.

Reading Hockey uses the Pitchero database to hold members’ data and Pitchero already has GDPR information. Their policies can be found [here](https://secure.pitchero.com/gdpr) . Reading Hockey Club’s privacy information can be found [here](http://www.readinghockeyclub.org.uk/policies/).

# GDPR

All volunteers must be aware of and understand the 6 principles of the GDPR to ensure that any processing of personal data you undertake as part of your volunteering duties is carried out correctly.

1. Lawfulness, fairness and transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Purpose limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Data minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy: Personal data shall be accurate and, where necessary, kept up to date.

5. Storage limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. Integrity and confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

## Accountability

One of the key changes with the GDPR is the accountability principle, which places greater responsibility on organisations to clearly explain and document why data is being collected and how it is being used. Reading Hockey Club’s data controller (the Webmaster) is responsible for determining the purposes for processing data i.e. how and why data is processed, and this is sanctioned by the Hockey Committee.

Volunteers, team managers, coaches and captains are not data controllers, and therefore cannot decide the purposes for processing data, and must comply with Reading Hockey Club’s processes and guidelines. Purposes of holding personal data are documented in the policies section the Reading Hockey website <http://www.readinghockeyclub.org.uk/policies/>.

Data protection is everybody’s responsibility. As a Reading Hockey volunteer, you may process data, as per the club policies, on behalf of the club. If so, you are responsible for looking after other people’s data.

If you stop performing a volunteer role, you should inform your club captain, membership secretary or webmaster of any data you have been managing and agree if this should be destroyed or handed over to another volunteer. You must not retain any copies of personal data.

# Reason for data collection & contact preferences

Reading Hockey Club collects members’ data for the purposes of servicing their membership, and we can contact members in relation to their membership, regardless of their contact permissions. For example, to invite members to play in matches or send renewal reminders. However, if we want to contact members about anything which is not directly related to fulfilling their membership contract – such as marketing from external companies - we can only do so if we have their consent to contact them.

We collect contact preferences and consent for non-membership related communications at the point of joining, and members can manage their contact preferences through their, or their child’s, account on the Pitchero database.

The Reading Hockey central database contains all members’ personal data and contact preferences. Contact preferences apply to all communications from Reading Hockey including those sent by team managers, coaches, captains and sections. Please ensure you follow these contact preferences and – importantly – do not contact members who have opted out of communications.

# Offline data

To help ensure you are compliant with GDPR, we strongly recommend that you only use the reports and lists provided by Pitchero to manage communications locally. Creating local data sets and lists could create confusion and lead to a data breach.

If you collect personal data, you are responsible for ensuring it is collected, managed and maintained in accordance with the GDPR. We therefore recommend that you refrain from collecting personal data from non-members or parents and ask member’s and potential members to use their Pitchero account or a form administered by the colts’ section.

If you use personal data in your role that is not held on your online Pitchero account, you must

* Ensure that data is stored securely and do not keep it longer than needed
* Use a password for any data stored on an electronic device
* Document your process in writing
* Register the data with webmaster@readinghockeyclub.org.uk informing what data has been downloaded, what purpose it is for and when it will be destroyed following the purpose of use

# Data of Under 18’s

The GDPR has very strict rules around how children’s data must be managed. All under 18’s at Reading Hockey must have parental permission to be a member of the club, have a parent record on the database in their own right and have contact information for two next of kin on the database.

Photographs of people are a type of personal data and all colts are asked if photographs may be used for the club’s purpose when they join. Guidelines differ depending on the purpose of the photograph, how many people are in it and if individuals are identified. Colts membership forms are stored by the Colts’ club captain.

Access to member’s data is managed through the Pitchero database. You will be given access to the data that you need to do your role. Access to the data should be closely controlled and not given to anyone else. If another club member or volunteer needs to have access to the data, please contact the webmaster at webmaster@readinghockeyclub.org.uk . You should only share offline data with other volunteers who have signed the GDPR data guidance form.

When sharing membership data with other volunteers, you must only share what is needed. You should also remind the volunteer that:

* they should be familiar with this guidance;
* they need to respect members’ contact preferences;
* they should destroy the data as soon as their activity is complete;
* be an ambassador for good data protection and support other volunteers.

# Member Accountability for their data

A key principle of the GDPR is that data must be accurate, so it’s very important that the Reading Hockey Club central database is the authoritative record of members’ details.

Members’ are expected to keep their own personal data up-to-date as part of the annual enrolment process and whenever their information changes. It should be updated by members in their own Pitchero record or by agreement with their team manager.

The quickest and easiest way for members to update their information is by logging into their account on the Reading Hockey website and changing their details in “My account” > Membership > Reading Hockey Club <https://secure.pitchero.com/account/membership/club/35901/>

If they do not have an account, they should be advised to create one at [www.readinghockeyclub.org.uk](http://www.readinghockeyclub.org.uk) > Join

# Membership activities based on Data Collected

To become a member at Reading Hockey Club each year, potential members need to enter, check and update their personal data. Reading Hockey Club match selection process runs on the Pitchero sport management system so all members do need to register. Players aged 13 and under will have their accounts managed by their parents. Players between 14 and 18 should register their account to receive emails to be able to manage activities alongside their parents.

It is OK for designated volunteers to maintain lists, eg a list that just contains names and contact details to manage registration, however just ensure you are clear about how an individual’s personal data is being used and stick to the GDPR principles around data minimisation, security and retention. Download only the data that is needed for the task that you are doing at the time. Please be very careful managing lists. If multiple local lists proliferate, it increases the risk of a data breach or incurring fines for poor data management practices.

If you are contacting members, please remember:

* You must use the most recent membership data supplied by the Pitchero database to ensure data is accurate.
* You must not contact members who have opted-out.
* Data lists should not be retained past the purpose for which they were obtained.
* Emails should go through the Pitchero system so that a clear opt-out option or unsubscribe message is present in all emails and contact preferences are adhered to.

If you have historical collections of data - for example, records of previous seasons, records of attendance at training events etc - please review whether you need to keep it for continued use at Reading Hockey Club or destroy it. If in doubt, please contact your club captain or the webmaster at webmaster@readinghockeyclub.org.uk.

# Subject Access Request

Under the GDPR, individuals can request to see their data. This is called a “subject access request”. If you receive one of these, please direct the member to their record on the database. If the member would like further information, please do not respond, but notify the webmaster webmaster@readinghockeyclub.org.uk within 24 hours who will advise on next steps.

# Security of data

## Personal devices security

Keeping your personal devices secure is one of the best ways to safeguard personal data stored electronically. Here are some simple things to remember to keep your electronic devices, and all the data on them, safe:

* Establish strong passwords and/or passcodes for all your electronic devices (laptops, personal computers, tablets and smartphones). Where possible, make sure you use a combination of letters and numbers for a hard-to-crack password.
* Keep laptops secure by using a username and a unique password. Make sure to never leave your laptop or any device where it is at the risk of being stolen or compromised, for example in a car.
* Use antivirus protection and anti-malware software. These serve as the last line of defence against unwanted attack through your network.
* Update your computer programmes regularly. Data security is enhanced with every update. Frequently updating your programs keeps you up-to-date on any recent issues or holes that manufacturers and programmers have fixed.
* Enable your device to lock after a short period of time. Most devices do this automatically, so after a set time devices “lock”. This is useful so that your devices are protected if you have to leave your screen for any period.
* Avoid using public PCs or laptops for official use as in most cases you are unable to verify the level of anti-virus or online security on the devices.

## Printing data

We recommend that you do not print out personal data or keep paper copies of data, as this is the least secure way to manage data. However, sometimes you may need to. In this case, make sure all physical copies are kept carefully and securely to avoid them being been seen or used by unauthorised people, stolen, tampered with or used for alternative purposes by any third party. To do this, keep data together in a file and ideally out of sight when not in use – for example in a drawer. As soon as the data is no longer needed, securely destroy the data by shredding. This is especially important for sensitive data.

Storing and archiving data is considered ‘processing’ of personal data, even if the data is not used or updated. Therefore, to comply with GDPR, personal data must be securely disposed of when it is no longer needed.

## Deleting data

Electronic data must be completely deleted when it’s no longer needed. If deleting data within a file, delete the data from the file, and then re-save the file. If deleting a whole file containing data, delete the file and then go to the Recycling Bin on your computer and delete the file from there too.

Any CDs and/or DVDs containing personal data must be cut up or crushed before being thrown away. When disposing of old equipment (such as PCs), please be mindful of data security. The only sure way to ensure that the drive contains no data is to destroy it. Devices that don’t have removable storage media, such as mobile phones, usually come with a function called something along the lines of ‘Restore to factory settings’ to wipe the data.

Paper documents should be shredded and put in the bin (not recycling) or disposed of using suitable confidential waste facilities.

# Security breach

A data security breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data and is an important new element of GDPR.

Examples of data breaches include:

* Mobile devices, briefcases and bags stolen from vehicles.
* A website with personal data being hacked.
* Documents with personal data missing after being left unattended.
* Used computers or mobile devices sold without first destroying personal data.
* Lost, unencrypted memory sticks and drives containing sensitive information.

If a breach has occurred, or you are worried one might have, please notify the webmaster webmaster@readinghockeyclub.org.uk within 24 hours who will advise on next steps. The club only has 72 hours to report the issue to the relevant authorities.

# Administrator Access to Pitchero

To gain administrative access to the Pitchero Database, all data controllers & processors should read the above, follow the training on Pitchero <http://www.readinghockeyclub.org.uk/a/website-training-47730.html?page=2> and sign to agree that they have completed both actions.

* I have read this document on GDPR and agree to abide by its guidance
* I have read the Pitchero training document on how to use the Control Panel

I am requesting access to view and process personal data for the following teams …………………………………………………..

Signed ………………………………………………………………………. Name ………………………………………………………….

Or reply by email to webmaster@readinghockeyclub.org.uk