Data Protection Subject Access, Request (SAR), Procedure and Guidelines

(Information contained herein is based on the ICO Data Protection Good Practice Note – Checklist for handling requests for personal information (subject access requests) and ICO Data Protection Technical Guidance Note - Dealing with subject access requests involving other people's information)

1.1 Roles During the Procedure

The Data Protection Officer (currently Operations Manager) will provide guidance, oversee and approve the request procedure. They will ensure that all electronic records are made available for the review, including:

Database records

Emails

Files

When a member of the club makes a request, a member of the Administration team would usually handle such a request, with the Data Protection Officer verifying the documentation before sending to the member.

If an employee has made the request, the Data Protection Officer will work with a member of the Board of Trustees in fulfilling and approving such a request.

1.2 Considering the Request

1.2.1 Is this a subject access request?

In many cases, a request for information or routine enquiry can be dealt with under the normal course of our work. These can be dealt with informally and there is no need to continue with this procedure.

A written enquiry that asks for information is likely to be considered as a subject access request. If it is likely that the request needs to be dealt with under this procedure or you are unsure, please speak to the Data Protection Officer at this point.

1.2.2 Are we sure of the requester's identity?

Often the member or employee is known to the organisation, and therefore, no proof of identity is needed.

If we have good cause to doubt the requester's identity, we can ask them to provide evidence we need to confirm it, such as a copy of passport, driving license or utility bill as part of the subject access request. The Data Protection Officer will discuss this with you.

1.2.3 Do we need any other information to find the records they want?

In the case that the member or employee asks for all information on file, we can reasonably ask the individual for more information to help assist in narrowing down the search, such as the dates they were involved with the organisation or if they are looking for something in particular.

However, the member/employee has the right to see all records and can restate that they would like this to be carried out.

1.2.4 Are we going to charge a fee?

Under GDPR rules, the club is typically unable to charge for a subject access request. Fee charging can be considered if the request is 'manifestly unfounded or excessive'. In these cases, the club is able to refuse to respond or levy a fee of up to £10. If the club refuses to respond, the club needs to be able to provide evidence of how the conclusion that the request is manifestly unfounded or excessive was reached.

In cases where the request is 'manifestly unfounded or excessive', the Data Protection Officer will decide whether to levy a fee or refuse to respond. It is the club's policy to try and respond to request where possible, accounting for time costs and resource capacity.

After making the decisions above, a subject access request can be made. Once this has been received, an acknowledgement letter will be sent to the member, along with details of the time limits.

1.3 Fulfilling the Request

When a staff member is handling a request, each document will need to be reviewed, and they must consider the following questions:

1.3.1 Does the file include any information about other people?

In fulfilling a request, we also need to protect the rights of third parties that may be involved in revealing the information to an individual. On each document, the following needs to be considered:

Does the request require the disclosure of information which identifies a third-party individual?

Has the third-party individual consented?

Would it be reasonable in all the circumstances to disclose without consent?

If you believe a third party should not be revealed. You may delete the name, titles or any other information that may reveal their identity, even if this results in withdrawing the whole document. Details of the reasons why will need to be responded to the person(s) making the request.

1.3.2 Are we obliged to supply the information?

There are certain circumstances in which we are not obliged to supply certain information. Some of these exemptions apply to:

Crime prevention and detection

Negotiations with the requester

Confidential references given by you (but not ones given to you)

Information used for research, historical or statistical purposes

1.3.3 Does the information include any complex terms or codes?

If the information includes abbreviations or technical terms that the individual will not understand, we must make sure that these are explained so the information can be easily understood.

A photocopy of all documents should be supplied. These must be sent to the Data Protection Officer for verification within 20 days. The time limit starts from when we have received the subject access request.

The Data Protection Officer will then verify all documentation and send it to the member or employee with a standard response letter within 10 days. All documents and correspondence should be kept as part of the internal record of the request.