The DATA PROTECTION ACT 1988
and How it affects Orienteering Clubs

1. **DISCLAIMER**: This document is provided in good faith as a guide to clubs. It has been seen by qualified and competent people and their suggestions have been incorporated. It is not a statement of the law and you should not rely on it to justify anything you may do or not do. If you have a query about your legal standing, contact one of the regulatory bodies or seek professional advice.
2. **Who should read this document?** Club membership secretaries, event organisers, those responsible for entries and results, club webmasters and all club and association officials who obtain, hold, use or publish personal data.
3. **Who is affected?** The Data Protection Act 1998 ("the Act") applies to all businesses, organisations and individuals who process personal data in any way (data controllers) and to individuals whose personal data is processed by others (data subjects), ie everyone.
4. **What is personal data?** Personal data means any information that relates to a living individual (the data subject), who can be identified from those data, or those data and other data in the possession of a data controller (. Personal data includes information such as name, address, email address, date of birth, telephone number, photographs where the data subject is identifiable and family details. Many people have concerns about their personal data being passed on to third parties, especially contact details.
5. **What does processing mean?** Within the meaning of the Act, this is obtaining, recording or even simply holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data. It is difficult to envisage any activity involving data that does not amount to processing.
6. **What does this document cover?** The requirements for clubs and associations to have a data privacy policy, ie how personal data will be obtained and used; to publish an appropriate summary of this policy with any paper or online form that asks for personal data; and to process the data according to various rules and safeguards. This includes membership data and event entry data. Most of the requirements will be readily understood as common sense respect for an individual's privacy and rights. Compliance with the Act is easily achieved and maintained, provided that all concerned understand their responsibilities under the Act. A general explanation of the Act is given in the Introduction, followed by specific requirements that clubs and associations must comply with. These do not detail every possible situation that may arise in connection with the Act, but there should be sufficient information for clubs and associations to make appropriate decisions. Some details of other regulations affecting online entry and web sites are also given. There is a summary of action to be taken at the end of the document.

1. INTRODUCTION

The Act imposes rules and safeguards on the use of all personal data, whether held electronically or on paper; the 1984 Act applied only to computerised records. The Act works in two ways.

- It says anyone who records and uses personal information (data controllers) must be open about how the information is used and must follow eight principles of good information handling.
- It also gives us all as individuals (data subjects) certain rights, including the right to see information that is held about us and to have it corrected if it's wrong.

The UK Information Commissioner (formerly Data Protection Commissioner/Registrar) maintains a public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data by a data controller. Individuals can consult the register to find out what processing of personal data is being carried out by a particular data controller. Notification is the process by which a data controller's details are added to the register.

Although individuals and some not-for-profit organisations are exempt from notifying the Information Commissioner of the data held and its use, there are restrictions for exempt organisations on what data can be held and how it can be used. Some orienteering officials may not be aware of these restrictions and their responsibilities. After several years of playing an educational role and acting on complaints received, the Information Commission is now pro-active, seeking infringements of the Act and prosecuting where necessary.

1.1. **Exemption for individuals:** If you process personal data for personal, family or household affairs (including recreational purposes), you are exempt from notification and most of the other provisions of the Act. This exemption does not allow you to publish personal data without permission of the data subject.

However, if you are processing data on behalf of your club or association, then you will be a "data processor". This means that your club or association is legally responsible for any processing that you carry out. You should therefore ensure that you carry out such processing in compliance with any instructions issued to you by your club or association and, in any event, that you follow the eight data protection principles set out in the Act.

1.2. **Notification exemption for not-for-profit organisations:** This exemption is intended for bodies or associations which are not established or conducted for profit. The normal activities of orienteering clubs and associations are likely to fall within this exemption criterion. You may choose to notify voluntarily, but this requires payment of an annual fee of £35. Although not-for-profit organisations are exempt from the notification requirement, such organisations are still required to process personal data in accordance with the provisions of the Act. Not all the exemption criteria are listed here, but *all* of your processing must be covered by the following descriptions. If there is any other processing, then you may not be exempt from notification. If you are in any doubt, you should seek professional advice.

Your processing is only for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are either members of the body or association or have regular contact with it.	Regular means that there is a regular arrangement, eg the standing agreement for members of other clubs and other national federations to enter events
Your data subjects are restricted to any person the processing of whose personal data is necessary for this exempt purpose.	Examples are: past, existing or prospective members (which includes members of the public entering events), members of other clubs competing in events, landowners and other supporting agencies, eg for first aid.
Your data classes are restricted to data that are necessary for this exempt purpose.	Examples are: names, addresses, categories of membership and competition, skills.
Your disclosures other than those made with the consent of the data subjects are	This includes publication of event results in the public domain and disclosure of data to

restricted to those third parties that are necessary for this exempt purpose.	certain individuals and organisations within the orienteering community necessary for the purposes of administering the sport (eg. BOF and the SOA.
The personal data is not kept after the relationship between you and the data subject ends, unless and for so long as it is necessary to do so for the exempt purpose	Archives of club newsletters and event results are allowed. Membership data for past members should be deleted from records after a reasonable period of time when it is clear that they will not renew membership (eg one year) or if the data subject requests that its data is deleted.

However, if

you are a limited company,
you have employees,
you make the data available to third parties outside the orienteering community, or
you use the data for any commercial gain,

it is likely that you must notify the Information Commissioner of your data usage. Seek professional advice.

British Orienteering Federation Ltd and the Scottish Orienteering Association have notified their data usage to the Commission. This notification does not extend to affiliated clubs or associations, which are separate legal entities. Neither BOF nor SOA do nor can exercise control over the processing of personal data by clubs and associations.

To reiterate: even if you are not required to notify, you (as a club, association etc.) are required to comply with the Act.

1.3. **Independent consultants:** There are consultants who offer genuine services to help develop policies and codes of practice. Some, however, send letters that appear to come from the Commission's Enforcement Department and threaten dire consequences if you do not register by completing an enclosed form and returning it with a large fee. There is normally no need for clubs or associations to notify. If you wish to do so voluntarily, the notification form is easy to complete and the Commission's Notification Department will give any assistance you need. The Information Commissioner's contact details are available at the end of this guide.

1.4. **What/who is a data controller?** This means a person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data is, or is to be, processed. Data controllers must comply with the provisions of the Act even if they are exempt from notification. In this document, responsibilities of the data controller are ultimately those of the club or association committee (and when adopting/referring to a data protection policy the data controller should be specified as the club or association), but specific duties may be delegated to one or more persons.

1.5. **The Data Protection Principles:** There are eight Data Protection Principles which determine what you may do. In summary, they require that data shall be:

1. fairly and lawfully processed,
2. processed for limited purposes and not in any manner incompatible with those purposes,
3. adequate, relevant and not excessive,
4. accurate,
5. not kept longer than necessary,
6. processed in accordance with the data subjects' rights,
7. secure,
8. not transferred to countries outside the EEA that don't protect personal data adequately.

2. COMPLIANCE WITH THE ACT

2.1. **Person responsible:** Although committees will make decisions on policy, it is good practice to appoint a person responsible for ensuring that the club or association complies with the Act, ie that all personal data, however obtained, stored and used, is processed in accordance with the Data Protection Principles. This person may conveniently be the membership secretary but can be any other member. The person responsible should read the relevant handbooks, codes of practice and checklists available from the Information Commission by post or via its web site — see Appendix 3.

2.2. **Data Privacy Policy**: Clubs and associations must have a Data Privacy Policy and communicate it to all members. This can be done conveniently by printing it as part of your membership application form. Ensure that it is on a part that the member keeps, eg with a list of membership benefits, not on the part that is completed and returned to your membership secretary. This brings it to the attention of all new members. For existing members, it can be published on a once-only basis in the club magazine or with any other document that is sent to all members. If the policy is subsequently amended, the new version must be communicated to all members. If you wish to use any existing data in a materially different way from the previous policy, you should obtain explicit consent from each member. A specimen Policy is given in Appendix 1. This will probably cover all use of data in the normal activities of clubs and associations. Note that some specific public disclosures of data are stated in the policy, eg publication of event entries and results, to ensure that members are made aware of this use.

2.3. **Membership and other forms:** Personal data must be obtained fairly and lawfully (1st principle) and must be adequate, relevant and not excessive (3rd principle). A key aspect of fair and lawful processing is the purpose for which the data is collected. This means that individuals must be made aware of the purpose for which they are supplying data, how it will be used and whom it will be disclosed to. Do not ask for data that is not needed for the purpose, eg the full date of birth when only the year of birth is required to determine the age class for competition. Membership application forms must have a data privacy statement stating what the club or association will do with the data and to whom, if anyone, it will be disclosed. It is good practice to use application forms to supply the full data privacy policy to new members. It is also best practice for all other forms which are used to obtain personal data also to have an appropriate data privacy statement. However, if a form is used only for the existing members of a club or association and they have previously received the policy, a statement may not be necessary, eg a booking form for a club dinner or an order form for club orienteering suits. Personal data may be used to provide a common benefit for all members, eg posting a club newsletter or providing a contact list to all members. An opt-in (ie a positive tick box) should be provided to give data subjects a choice as to how their data is processed and forms should therefore provide for this. You may also wish to use a separate opt-in for essential and non-essential processing (ie processing other than simply for administrative purposes versus group emails and mailshots about forthcoming events). For example, you must not assume that members wish to receive news by email just because they have provided an email address as a means of contact. Best practice is always to use an opt in. You must ensure that members can confirm that they still require such a service at regular intervals. This can be done by including an ‘opt-out’ or unsubscribe option at the end of such emails, by including a notice periodically in your club newsletter and by including opt-out details in your data protection policy. Forms must include, or be accompanied by, contact details for the data controller and, if appropriate, the person responsible for processing data on the data controller’s behalf.

2.4. **Data accuracy:** You must take reasonable steps to ensure the accuracy of the information (4th principle). In most cases, data will be provided by the data subject or a family member. As membership is renewed annually, the data subject is able to check and inform you of any changes. If copies of data are in use, one person must be responsible for accuracy of a master record and ensure that those who use copies are kept up to date. This means in practice that clubs should ensure that membership and contacts databases are maintained by **one** individual, who is responsible for ensuring that such databases are up to date, and that updates of these databases are then disseminated as necessary to other members/officials who reasonably **require** access to such data (see 2.5 below).

2.5. **Data security:** You must take measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data (7th principle). You need to establish who is entitled to access data. Keep a record of what data is held by which officials and members so that you can ensure changes are given to all who need to know and can provide access to the data if requested by a data subject. Many clubs distribute all contact data to all members to assist in sharing of transport to events and to enable event officials to recruit volunteer helpers, and some members might not want their details included. When a contact list is supplied to members, they must be reminded to destroy any previous version securely. Other data may be needed by officials to carry out their duties. Some data may need to be shared with other orienteering organisations (such as BOF and the SOA) to provide the services that members require or to meet the requirements of governing bodies. However, disclosure of data to other third parties will require the data subject's explicit consent if the organisation has not already obtained this. It must be made clear to all individuals with access to the data that they must not disclose personal data without consent. Where data is stored on a computer, there should be provision for a regular backup copy to secure against accidental loss or corruption and an anti-virus program should be used and kept up-to-date to secure against corruption or misuse by viruses and other malware. If other persons have access to the computer but are not authorised to access the data, access to the data should be protected by password. Reasonable steps must be taken to protect the computer and copies of data from theft. Note that personal data may be included in correspondence and notes as well as formal records. Ensure that all officials are aware of information security issues. Where personal data is transmitted by email, ensure that it is sent only to those authorised to access it. In particular, when issuing club/association-wide emails, ensure that the display of email addresses to multiple correspondents is suppressed in the received email by using the blind copies field (Bcc) or other available functions in the email program.

2.6. **Data retention:** This concerns retention of data about prospective, current and past members (5th principle). The data controller should set retention periods. No specific period is given in the Act, which merely requires that the personal data in a record shall not be kept for longer than is necessary for a particular purpose or purposes. Newsletters, magazines and event results will contain personal data published as permitted disclosures and may be kept as archives. Membership data should be destroyed when it is clear that a member will not renew membership. It is common for members not to renew due to serious injury or to working away from home for an extended period and to take up membership again when recovered from the injury or returning home. A retention period of two or three years may be considered reasonable. Event entry data should be destroyed after a period allowing for protests and appeals against results, say 3 months after results publication or any protest or appeal is concluded. Accident and insurance forms and reports may need to be kept for longer periods. Ensure that records for disposal are destroyed securely and effectively, including any copies.

2.7. **Data transfer and public disclosure:** Data must not be transferred to countries that don't protect personal data adequately (8th principle). European Economic Area

(EEA) countries have appropriate data protection legislation. The USA does not. There is usually no need to transfer data to other countries, except for that displayed on web sites. Any agent used for processing event entry or transacting online payment will normally be UK-based. If a club enters members for an event or arranges travel or accommodation in another country outside the EEA, then data may be disclosed only with the consent of the member. Personal data displayed on web sites is public. Care must be taken to ensure that any data displayed is acceptable to the data subject. This will normally be so for offices held, event entries and results published in the commonly used formats. However, most members are sensitive about displaying contact data, especially email addresses. Explicit consent should be obtained before displaying such data. Note that this also applies to contact data in fixture lists and event advertisements — some members have complained about some details disclosed without consent. Public disclosure of any contact data for children must be carefully considered and parental consent must be obtained. This is most likely to occur when a junior member is an event organiser.

2.8. **Sensitive data – instructors and coaches:** These officials may need access to personal data classed as sensitive — see Appendix 2. They may be acting in loco parentis for minors or may need to know about diet, blood group, allergies, injuries and other health data in case of accident or illness and to provide competent and responsible coaching advice. Obtaining and using such data requires the explicit consent of the data subject, parent or guardian. A positive indication of agreement must be given, eg a signature. Strict confidentiality and security of the data apply. The subject must be given a clear privacy statement including who has access to the data. As with personal data, where the instructor or coach is acting within and on behalf of his/her own club or association, that organisation is responsible for compliance. If a coaching arrangement is a personal one between the data subject and instructor or coach, there must be explicit consent by the subject. If the arrangement is a commercial one, ie the coach receives payment for the service provided, other than out-of-pocket expenses, then the coach may not be notification-exempt, consider notifying the Information Commission voluntarily.

2.9. **Sensitive data – accident records:** Sensitive data may also be required for the completion of accident and insurance forms and reports. Explicit consent is required and care must be taken to ensure this when a casualty is not fully aware of what is happening. A positive indication of agreement should be given, eg a signature. Strict confidentiality and security of data apply.

2.10. **Data subject's rights:** Data subjects have rights (6th principle) to:

- be informed upon request of all the information held about them by a particular data controller;
- prevent the processing of their data for the purposes of direct marketing;
- compensation if they can show that they have been caused damage by any contravention of the Act;
- the removal or correction of any inaccurate data about them.

2.11 **Data subject's access:** The Act gives individuals a right of access to their personal data. Upon making a written request and paying the requisite fee, an individual is entitled to have communicated to him in intelligible form:

- a copy of the information which forms any such personal data, and
- a description of why this information is processed, and
- anyone it may be passed to or seen by, and
- the logic involved in any automated decisions, and
- any information available to the data controller as to the source of the data.

The data controller must respond promptly, at most within 40 calendar days of receipt of the request and fee. As well as the obvious records of membership, event entries and results, there may exist officials' correspondence and notes that contain

data about the subject. Searching emails and computer files is straightforward, but a search for all such data on paper may take some considerable effort and a subject access request will only catch paper records if they form part of a "relevant filing system". A relevant filing system is one which is organised in such a way as to allow someone to instantly find particular pieces of personal data and accordingly very few paper-based filing systems will be covered. Recent case law suggests that personal data (whether in electronic or paper form) should be biographical in nature rather than simply referring to the data subject and, for instance, the inclusion of a data subject's name in a letter does not necessarily mean that the letter is caught by a subject access request. This is an evolving area of the law and in the event that you are unsure whether you should disclose a document, you should seek legal advice. Relevant documents may contain data about third parties who also have a right of privacy, so it will be necessary to obtain their consent or edit such correspondence before supplying it, in order to protect the third party's rights. If the third party does not give his or her consent, you can 'redact' the data – ie anonymise – prior to disclosure. The data subject may not wish to receive copies of all or some of these documents — ask. The information may be provided at no charge or a fee may be required to contribute to the expense of searching and providing the data and to deter frivolous requests. A standard fee, not exceeding £10, must be determined by the data controller. Because of the open and transparent way in which most clubs are organised, it is unlikely that such requests will occur.

2.12 Objections to processing: Section 10 of the Act sets out the general right to object:

… an individual is entitled at any time, by notice in writing to a data controller, to require the data controller at the end of such period as is reasonable in the circumstance to cease, or not to begin, processing or processing for a specified purpose or in a specified manner, any personal data of which he is the data subject, on the grounds that, for specified reasons:
(a) the processing of those data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or another, and
(b) that damage or distress is or would be unwarranted.

Points to note are that objections must be in writing, and that the grounds for objection are limited to cases where there is or is likely to be substantial and unwarranted damage or distress to the data subject or another person. There will be cases where it is good practice to act upon an objection made by means other than writing. It would also be good practice to respect an individual's wishes even if they could not demonstrate that the damage or distress caused to them was substantial. A data controller in receipt of a written objection to processing must, within 21 days, inform the person making the objection in writing whether it has complied or intends to comply with the request or must state its grounds for refusing to do so. The Act gives no comprehensive guidance as to valid grounds for objecting to the processing of data, although it makes clear that the interests of the data controller will outweigh those of the person objecting to the processing of data if the processing is on the basis of any of the following four conditions:

- The data subject has given his consent (this condition will be relevant where the person objecting to the processing is a person other than the data subject);
- The processing is necessary for the performance of a contract or for entering into a contract at the request of the data subject;
- The processing is necessary for compliance with legal obligations (for instance a disclosure made on a statutory basis);
- The processing is necessary to protect the vital interests of the data subject (this condition will also only be relevant where the person objecting to the processing is a person other than the data subject).

A data subject also has the right, under section 11 of the Act, to object to processing for the

purposes of direct marketing. Direct marketing means communication (by whatever means) of any advertising or marketing material which is directed to particular individuals (see also Other Relevant Legislation below, which deals with electronic communications).

3 EVENT ENTRIES

3.1 Multi-day events: The British Championships weekend and JK are organised on behalf of BOF by area associations. The association's Data Privacy Policy will apply but it may be convenient to appoint a Data Privacy Officer specifically for the series of events. For event series undertaken by a group of clubs, eg the Scottish Six Day, the SOA is not responsible and the organising group (the Six Day Company) must decide its own policy and other arrangements for the series.

3.2 Event advertising: In addition to the Act, the Electronic Commerce (EC Directive) Regulations 2002 apply to anyone who advertises or sells goods or services online. Also, the Consumer Protection (Distance Selling) Regulations 2000 apply when goods or services are ordered by telephone, post or online. For the latter, leisure services including outdoor sports events are partially excluded, but if you are selling goods at the same time, such as a souvenir mug or T-shirt to be ordered by telephone, post or online, then they do apply in full (including the right to cancel). Fixture lists and event leaflets vary in purpose and the amount of advertising detail offered. Some examples illustrate the requirements for compliance. For those giving minimal information, eg date, venue and a contact, it is not necessary to provide a data privacy statement. The intention is that a prospective entrant will make contact to obtain further details which will include all required information. For fixture lists which include an address for sending entries, sufficient information must be provided to enable an entrant to use the BOF Standard Entry Form and send the entry form and fees by post. This form has the appropriate data privacy statement. If a special entry form is used, the statement must be included with that form. For details of the information required, see section 3.4. For leaflets advertising an event, you need not include a privacy statement, as it will be provided at the event or with the entry form, but you must include contact details for the event organiser or person responsible for processing entries. Under the Distance Selling Regulations, you must allow a 7-working day cooling-off period for any goods ordered, from receipt of the goods, during which the entrant can cancel the order without penalty.

3.3 Event entry on the day: It is usual for details to be recorded by an official without the use of an individual entry form. A copy of your Data Privacy Policy or appropriate summary should therefore be prominently displayed at the place of entry prior to competitors entering.

3.4 Event entry in advance: It is necessary to provide sufficient detail with the event entry form and instructions. A brief summary statement, informing entrants how the data will be used and its retention period, should be included on all forms. For most orienteers the use of the data may be obvious, but by stating how it will be used, you are also implying how it will not be used. This may be more significant, eg you are not passing it on to a third party. Statements about storing or processing data on computer, as commonly used, are not relevant — the crux of the matter is what the data is used for and to whom, if anyone, it will be disclosed, not the means of storage or processing. The following specimen statement should suffice:

*DATA PRIVACY: The personal data you give will be used by the [*insert name of the data controller*] only for the purpose of processing and publishing entries and results for [this event]. Entry data will not be retained after [three months] from results publication or the conclusion of any protest or appeal. By entering this event, you hereby give your consent to the use of your personal data for these purposes and the inclusion of your name and other details in any results or reports (including media reports and press releases) produced by us following this event.*

The retention period must be set by the data controller. If you wish to do anything more with the data, eg send mailings about future events, you must give details and allow the entrant to give explicit permission, ie opt in. However, it may be better to avoid extending

the use of entry data as it requires additional effort in providing the safeguards to control such use. The entrant must be given contact details for the person responsible for processing entries. Fixture lists and event advertising leaflets usually have this information. You must ensure that they have a geographic postal address and phone number. If a third party agent is used to process entries, ensure that it complies with the Act. See section 3.7 below.

3.5 Online event entry: There are additional requirements for web sites. Although some sites are hosted and maintained on a voluntary basis, the requirements are easy to comply with and once the necessary notices are added to the site, the club's webmaster should have no difficulty in keeping the site compliant. You should display your Data Privacy Policy in full. The Policy should either be on the home page with equal prominence to other items on the page, or, more conveniently, on a separate page with a link from the home page that is equally as prominent as other links. Do not use a small font. Your site should display contact details for your webmaster and the data controller which are either on or accessible from the home page. There should be a geographic postal address for the data controller. For this purpose, the data controller may be the organisation's secretary or a person appointed for that role. Always let users know when and why you intend to use cookies. If you use your website to capture data (eg through enquiry forms etc), a link to privacy policy a statement saying "I accept the terms of the privacy policy" with a tickbox should be included immediately above the "submit" button. This ensures that visitors to the website are made aware of the terms of the privacy policy before submitting information. Also display contact details for the person responsible for processing that data, eg entries secretary or event organiser. If you intend to collect and use data for mailing (by post or email), in addition to that necessary for the event, ask explicit consent to do so — the entrant opts in. Note that this may require additional effort to set up safeguards that ensure proper control. If you link to a third party agent to process the event entry, that agent must also display its own Data Privacy Policy and similar notices and statements on its web site. These must be accessible during the entry process. It must be clear that a third party agent is being used. If payment for entry is to be made only at the event, the online entry will normally be a reservation service only for allocating start times. This is typically used for Colour-coded events. The financial transaction has not been concluded and a contract is made only at the time of payment. If it is intended that payment of an entry fee is binding on the entrant, then this must be stated in the terms and conditions and the requirements of the following section on online payment apply.

3.6 Online payment: All the above online entry requirements *must* be complied with. In addition, the Electronic Commerce (EC Directive) Regulations 2002 apply to anyone who advertises or sells goods or services online and the Consumer Protection (Distance Selling) Regulations 2000 apply if goods are ordered online. These require you to:

- display full contact details: name, geographic postal address (ie not a postbox address), email address, phone number and, if applicable, VAT registration number
- state the different technical steps to be followed to complete the entry or order before starting the process, to make sure that the user is aware of what it will involve,
- display full contact details: name, geographic address (ie not a postbox address), email address, phone number and, if applicable, VAT registration number, and they must be easy to find,
- state entry fees, and the prices of any other items such as sending results booklets or fees for changing courses, in a clear and unambiguous way; including the words 'Event organised under BOF Rules' is sufficient to avoid the need for lengthy details of all courses and age classes,
- state how the user can check for and correct any input mistakes in both event entry and payment data before they are submitted,
- if goods are also being ordered, state details of the 7-day cooling-off period, during which the user can cancel the order without penalty, and how the user may do so,

- state any terms and conditions, such as reserving the right to retain all or part of the entry fees should the event be cancelled, before the payment data is submitted (the point at which a contract is entered),
- make these terms and conditions available in such a way that the user can store them for
- viewing or printing at a later date, acknowledge receipt of the entry, and order if appropriate, to the user without undue delay and by electronic means, either online at the end of the transaction or by an email that clearly identifies the sender.

Any third party agent you link to for transacting the payment must also display its own Data Privacy Policy and similar notices and statements on its web site. These must be accessible during the transaction process. It must be clear that a third party agent is being used. Such a commercial service may have to notify the Information Commission.

3.7 Responsibility for third party agents: If you contract with another third party to process data on your behalf, you should ensure that you have a written agreement in place covering the use of any personal data that you provide to that data processor. As the data controller, it is your responsibility to ensure that the data is being processed in accordance with the Data Protection Principles. In many cases, it is likely that the third party (for instance the provider of a secure payment facility) will have appropriate wording in its standard terms and conditions, as it is in that third party's interest to ensure that it is not responsible for complying with the Act and is simply acting under your instructions. In some cases, it may be necessary for both parties to be data controllers and in such situations each party will be independently responsible for ensuring that its processing is carried out in accordance with the Act and the Data Protection Principles. If you are unsure as to who should be the data controller or whether you have an appropriate agreement in place, you should seek advice.

4 OTHER RELEVANT LEGISLATION

The EC Directive on Privacy and Electronic Communications (2002/58/EC) came into effect from November/December 2003. Amongst other things, this clarifies the position of e-mail and internet use by

- extending controls on unsolicited direct marketing to all forms of electronic communications including unsolicited commercial e-mail (spam) and SMS to mobile telephones; spam and SMS will be subject to a prior consent requirement, so the receiver is required to agree to it in advance;
- introducing controls on the use of cookies on web sites and similar tracking devices which will be subject to a new transparency requirement — anyone employing these kinds of devices must provide information on them and allow subscribers or users to refuse to accept them if they wish.

This means that advertising events by email is not permitted unless previously requested, but event details sent only to their entrants or any information sent to subscribers to an opt-in news service are permitted. In addition, unsolicited emails etc must contain certain information about the sender and should explain to the recipient how it can opt out of receiving further communications.

The law related to use of “cookies” on websites changed in May 2011. You are now required to state what information you collect from users of your website. Usually this can be done by a popup message, and continued use of the website can usually be taken as implied consent. See the Information Commissioner’s Office website for more information.

5 SUMMARY OF ACTION

1. Appoint a Data Privacy Officer, responsible for ensuring compliance with the Act.
2. Formulate a Data Privacy Policy and communicate it to all members.
3. Follow the Data Privacy Policy and ensure that all processing is carried out in accordance with the eight data protection principles.
4. Include an appropriate privacy statement on all paper forms which collect personal data.
5. Display an appropriate privacy statement at all events where people enter on the day.
6. Display your Data Privacy Policy on your web site with a link from the home page. It is good practice to do this even if you do not yet have any online data entry.
7. Display contact details for your webmaster and your Data Privacy Officer either on or accessible from the home page.
8. On any web page where personal data is entered, display the purpose and an appropriate privacy statement with a link to your Data Privacy Policy page.
9. Ensure that those who enter personal data have to acknowledge your Data Privacy Policy before submitting the data.
10. If you use third parties to collect online data or online payment, check that their web site complies with the requirements of the Act and, if applicable, that they have notified the Information Commissioner.
11. Keep a record of what data is held by which officials and ensure that they understand their responsibilities according to the eight principles.
12. Determine a standard fee for subject access requests.

APPENDIX 1

This specimen policy has more detail than the Act requires, so that members can understand fully what happens to their personal data. To adapt it for your own use, replace '<club>' as appropriate. This specimen is also available as a Word document.

DATA PRIVACY POLICY (SAMPLE)

The Data Protection Act 1998 imposes rules and safeguards on those who hold and process personal data, ie data relating to living identifiable individuals. Details of usage must be notified to the UK Information Commissioner, with some exceptions which include not-for-profit organisations whose usage is restricted to specified purposes. <Club> is exempt from notification but the principles setting out rules and safeguards do apply. In the interests of being open and fair, <club> wishes to inform members of the data held and how it is used. <Club> and its officials may hold some or all of the following data about some or all members and others who compete in orienteering events: name, postal and email addresses, phone and fax numbers, year of birth, competition age class, competition results, offices held, skills and qualifications, courses attended and details of officiating at competitions. Contact data is held for landowners and other organisations with whom we co-operate with from time to time, their employees, agents and tenants. The data may be held in electronic or paper form.

The data may be obtained directly from an individual person or a family member or indirectly from the British Orienteering Federation, the Scottish Orienteering Association, other clubs or other organisations.

The data is used for administrative purposes in organising the sport of orienteering and for social and other purposes, including, but not limited to, mailing of magazines and other literature, publication of competition entries and results, coaching, team selection, training and appointment of officials. Data may be distributed in paper or electronic form between members, competitors and orienteering organisations. Publication of personal data in paper form may occur in membership and contact lists, magazines, competition information and results and other literature. Publication on publicly accessible web sites may include name, age class and club in competition results; names with offices and photographs may be published, but addresses, contact numbers and personal background details will be published only with the explicit consent of the person. Other than for the purposes of establishing or maintaining membership of or support for <club> and the sport of orienteering, or providing or administering activities for individuals who are either members of <club> or who have regular contact with it, <club> will not disclose personal data to any third party without the data subject's prior consent..

The data will not be available for commercial purposes.

If you do not wish to receive mailings (by email, post or other means) or other non-administrative communications from <club>, or you believe that the data held by <club> about you is incorrect, please contact <club>'s data protection officer, [name] at [insert contact details].

APPENDIX 2 – Sensitive Personal Data

What is sensitive personal data? The Act sets out a series of conditions, at least one of which has to be met before a data controller can collect, store, use, disclose or otherwise process sensitive personal data. For clubs and associations, as notification-exempt organisations, the only relevant condition is if the data subject gives explicit consent. Sensitive data is information concerning an individual's

- racial or ethnic origin,
- political opinions,
- religious beliefs or other beliefs of a similar nature,
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- physical or mental health or condition,
- sexual life,
- commission or alleged commission of any offence, or
- proceedings for any offence committed or alleged to have been committed, the disposal
- of such proceedings or the sentence of any court in such proceedings.

APPENDIX 3

SOURCES OF FURTHER INFORMATION:

Information Commissioner's Office (Scotland)

Information Commissioner's Office
45 Melville Street
Edinburgh
EH3 7HL

Tel. 0131 244 9001
Email: scotland@ico.org.uk

Their English office is at:
Wycliffe House
Water Lane
WILMSLOW
SK9 5AF
Telephone: 0303 123 1113 or 01625 545745
or contact via their website: http://ico.org.uk/

Department of Trade and Industry Enquiry Unit

1 Victoria Street
LONDON
SW1H OET
Telephone: 020 7215 5000
Contact via their web site:
http://www.dti.gov.uk

Some useful guidance:

Guidance on use of cookies:
http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies

Distance Selling Regulations guidance:
https://www.gov.uk/online-and-distance-selling-for-businesses
Advice on the regulations is also available from your local authority **Trading Standards Department**.

Document History

		Review due
Version 1	To SOA website 10/2/2005	Feb 2008
Version 2	for SOA Board approval May 2013	

Document drafted and maintained by
Hilary Quick