General Data Protection Regulation

CNCC Briefing for Caving Clubs, April 2018

Contents

Section One: Introduction

All caving clubs should consider taking steps to be as compliant as is practical with the EU General Data Protection Regulation (GDPR) by 25th May 2018.

To do this they are recommended to:

- Communicate their GDPR (Data Protection) policy (see example in Appendix A) to all members.
- If required, gain the members consent to hold their data. There is a section below on consent which explains why this must be done, how and when.
- Create a data protection policy (see example in Appendix C).

Potentially fines for failure to comply with GDPR are up to €20 million, or 4% annual global turnover, whichever is the higher! It is therefore the recommendations of the CNCC that all caving clubs consider carefully the implications of GDPR with respect to any members data that they hold and act accordingly.

Useful resources

We have been helped and guided by the BMC's advice: https://www.thebmc.co.uk/gdpr-mountaineering-clubs:

The following may also prove to provide a useful resource: https://www.sportandrecreation.org.uk/pages/gdpr

The BCA have recently (April 2018) posted their privacy notice:
http://british-caving.org.uk/wiki3/doku.php?id=about:documents:privacy_notice

The formal advice from the Information Commissioner (ICO - the UK Data Protection Authority) "Guide to the General Data Protection Regulation (GDPR)" can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

Finally, some information on processing of personal data: consent and legitimate interests under the GDPR can be found here: https://www.slaughterandmay.com/media/2535723/processing-of-personal-data-consent-and-legitimate-interests-under-the-gdpr.pdf

Disclaimer

The content of this document is a commentary on the GDPR, as we (CNCC), interpret it, as of the date of publication. This content is provided for informational purposes only, to help serve as general guidance, and should not be relied upon as legal advice or to determine how GDPR might apply to your club.

Section Two: GDPR Compliance

To comply to GDPR, organisations need to embed six privacy principles within their operations:

1. Lawfulness, fairness and transparency

Transparency: Tell the subject what data processing will be done. Fair: What is processed must match up with how it has been described. Lawful: Processing must meet the tests described in GDPR.

2. Purpose limitations

Personal data can only be obtained for "specified, explicit and legitimate purposes". Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

3. Data minimisation

Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". In other words, no more than the minimum amount of data should be kept for specific processing.

4. Accuracy

Data must be "accurate and where necessary kept up to date". Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data (i.e. a means to ensure the data is kept up to date).

5. Storage limitations

Regulators expect personal data is "kept in a form which permits identification of data subjects for no longer than necessary". In summary, data no longer required should be removed.

6. Integrity and confidentiality

Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage". In other words, the data should be in a secure place and accessible only by those who absolutely need to.

Issues Arising from the GDPR Compliance Requirements

Assuming your club Secretary manages the membership list in a competent manner in accordance with the privacy principles; the main issues are:

a) Establishing a lawful basis for processing, e.g. use legitimate interests and/or gain consent?
b) Data storage: is it GDPR compliant (i.e. in the European Union, secure and well backed up)?
c) Dealing with withdrawal of consent or objections
d) Sharing addresses amongst members

a), c) and d) are dealt with in this document, whereas b) should be addressed as part of a separate information security policy. It is assumed that clubs process personal data (names, address and other contact details) but not sensitive data (medical conditions, ethnicity).

Checklist

There is a web version at: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/controllers-checklist/

Mandatory

Your data protection policy will probably include a simple information security policy and will need to demonstrate you have carried out the following activities:

1. You have organised an information audit identifying and documenting any risks you have found (e.g. storing data on an unbacked up machine).
2. You have documented what personal data you hold, where it came from, who you share it with and what you do with it. Think about what data you are holding for your members; names, addresses, email and phone numbers, DOB, bank details, next of kin, medical details etc. Is it all necessary?
3. You have identified your lawful bases for processing and documented these data.
4. If you are using 'consent' as the lawful basis for processing:
    a. You have reviewed how you ask for and record consent
    b. You have a system to record and manage ongoing consent
5. If you are relying on 'legitimate interests' (see below and appendix B) as the lawful basis for processing these data, you have applied the three-part test and can demonstrate you have fully considered and protected individual's rights and interests.
6. You have let your members know why you are processing their data and who you share it with.
7. You have created a process to recognise and respond to individuals' requests to access their personal data.
8. You have created a process to ensure that the personal data you hold remains accurate and up to date.
9. You have implemented a process to securely dispose of personal data that is no longer required or where an individual has asked for it to be erased.
10. You have procedures to respond to an individual's request to restrict the processing of their personal data.
11. You have procedures to handle an individual's objection to the processing of their personal data.
12. You have an appropriate data protection policy. Make sure it is available to your members.
13. You are actively monitoring compliance to your data protection policy.
14. You are providing data protection awareness training for all individuals using club data (e.g. Committee).
15. You have a written contract with any processors you use.
16. You manage information risks in a structured way so that the club committee understands the business impact of personal data related risks and manages them effectively. Consider how secure your data is. How safe is your website? Consider obtaining an SSL Certificate (contact the CNCC webmaster for advice). How do you email your members? Do you always use 'Blind Carbon Copy' (BCC), and could a more bespoke online email system perhaps be better, more secure and less open to accidental disclosure? Who has access to the data and can this be justified for everyone who has access?
17. You have implemented appropriate technical and organisational measures to integrate data protection into your processing activities.
18. You have an information security policy supported by appropriate security measures.
19. You have a process to identify, report, manage and resolve any personal data breaches.
20. If there are any further changes to how you use the data you have, your data protection policy, or the type of data that you collect/store, you have a mechanism in place to obtain reconsent from your members to hold their data. Do not assume continued consent if there are any changes.

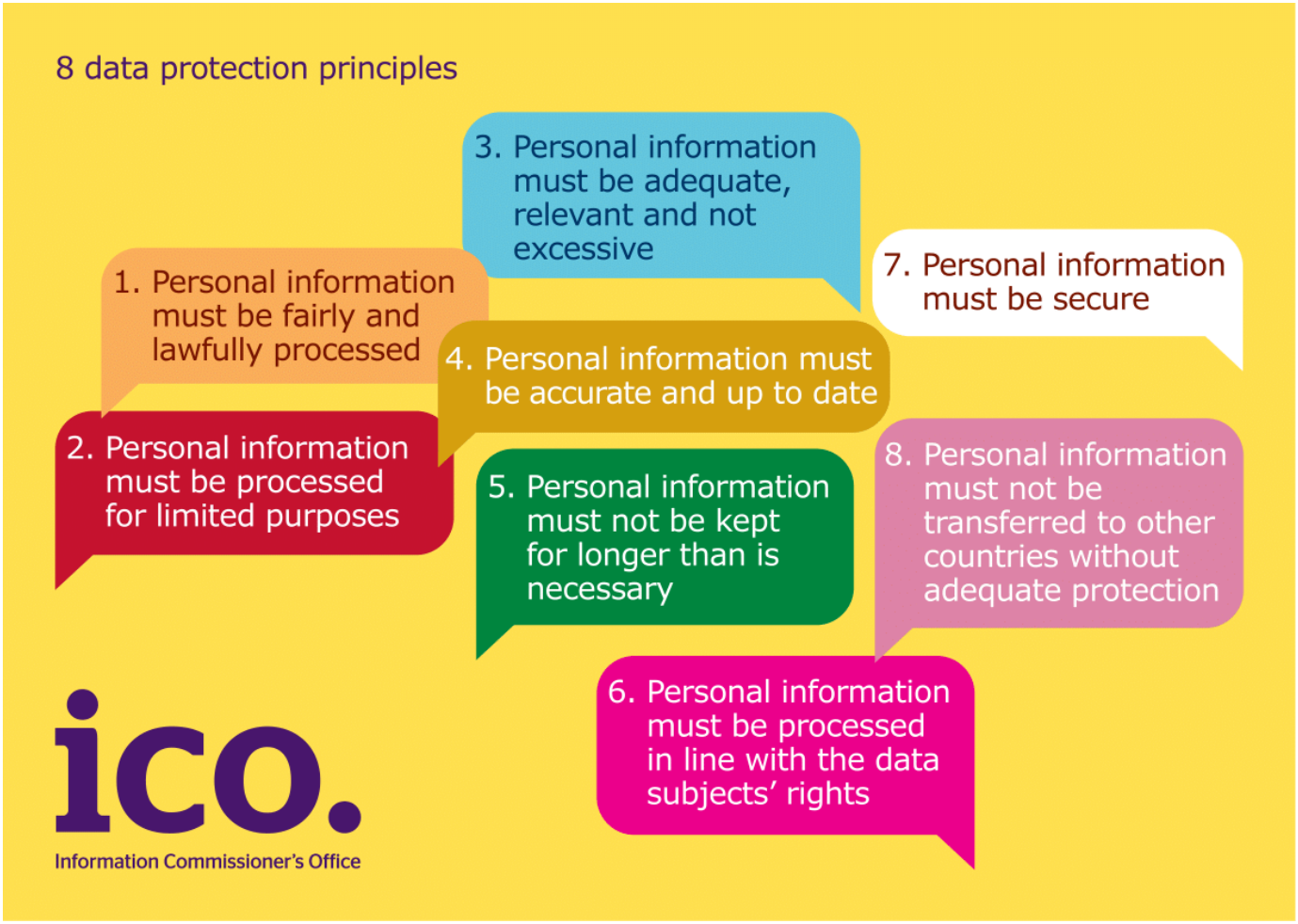
If required (may not be relevant for a caving club)

1. You have a process to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability [in fact mandatory but almost certainly irrelevant]
2. You have paid the data protection fee to the Information Commissioner's Office (see registration requirements below)
3. You have identified whether any of your processing operations constitute automated decision making
4. You carry out a Data Protection Impact Assessment
5. You have appointed a Data Protection Officer (may be required as a result of your DPIA)
6. You ensure an adequate level of protection for any personal data processed by others on your behalf that is transferred outside the European Economic Area

See: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ and https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

Registration Requirements

Under the old Data Protection Act most clubs did not have to register, but had to act in accordance with the eight Data Protection Principles:



This is because most clubs are non-incorporated associations. If you are a not for profit company, you will likely have registered as a data controller.

The relevant statutory instrument for the current Data Protection Act is SI 2000 no 188; The Data Protection (Notification and Notification Fees) Regulations 2000, schedule 5 sections a) and b)

http://www.legislation.gov.uk/uksi/2000/188/made

These sections should exclude non-incorporated associations (most caving clubs) from the need to register under The Act on the basis of not-for-profit and that the data is for the purpose of maintaining membership.

There is no requirement to register with national data controllers under the EU GDPR.

Most Caving clubs are not-for-profit organisations and it is likely that they will not have to register for Data Protection with the Information Commissioner, but you are advised to check yourselves by using the self-assessment facility on the website of the Information Commissioner's Office (ICO):

https://ico.org.uk/for-organisations/register/self-assessment/.

Scotland

Scotland has a separate Information Commissioner who does not appear to have issued separate advice.

GDPR Rights

The new EU GDPR has, like the preceding Data Protection Act, "rights" attached to it.

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Rights 1-7 are addressed in the policy statement, right 8 is not relevant. This will be covered in more detail in the example Data Protection Policy.

Section Three: Lawful Bases for Processing Data

There are six lawful bases for processing that are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

d) **Vital interests:** the processing is necessary to protect someone's life.

e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Legitimate Interest

This bases for processing data is likely to be of use to many caving clubs. The following is from the BMC guidance:

> *Legitimate Interest is likely to be most appropriate where you use people's data in ways they would reasonably expect [such as being a member of a club] and which has a minimal privacy impact [i.e. you only use the data for contacting the member about their annual renewal, the club meets programme, the club AGM, passing data to the* [BCA] *for membership administration].*
>
> *You must balance the interests of your club against the interests of your members. If your members would not reasonably expect the processing of their data their interests are likely to override the clubs legitimate interests. [i.e. if you start contacting them about other activities such as a promotion at a climbing wall, or you circulate their details in a members contact list].*
>
> *To use legitimate interest, the processing of your members' data must be necessary, but if you can reasonably achieve the same result in another, less intrusive, way then legitimate interest will not apply.*
>
> *A Legitimate Interests Assessment (LIA) needs to be completed before relying on this basis for processing data, and a record needs to be kept to help you to demonstrate compliance. You must also include details of your legitimate interests in your privacy notice. It is possible to claim legitimate interests as a basis and the BMC has produced advice for using this route.*

However:

- ***legitimate interests*** sometimes require consent; e.g. if you share contact details amongst members (which thus goes beyond what might be reasonably expected or what is minimally necessary for running the club or processing and effecting that individual's membership).

- Individuals have the ***right to object*** to processing based on ***legitimate interests***. BCA insurance is a requirement for membership in most caving clubs and clubs cannot give members the right to opt out from BCA insurance and the data processing this implies.

- If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected.

An example of the use of legitimate interest as a lawful basis for holding and processing most club data is provided in appendix B.

Consent

Consent requires a positive opt-in. Just being a member of a club and paying your subs is NOT a sufficient basis. You will require consent if you share **ANY** membership details between members; including the use of email lists in which email addresses of other members can be seen by the recipients. Consent must be specific and informed. Everyone must be re-consented and previous consents do **NOT** constitute a legal basis for processing data. The club Secretary **needs to be able to prove** that all members have given their consent.

The (Information Commissioners Office) ICO sets out the following guidelines for managing consent:

- Consents are regularly reviewed to check that the processing and the purposes have not changed.
- Processes should be in place to refresh consent at appropriate intervals, including any parental consents.
- It should be easy for individuals to withdraw their consent at any time and publicise how to do so.
- Withdrawals of consent are acted upon as soon as possible.
- *Individuals who wish to withdraw consent are not penalised.*

This means that **clubs do not have to renew consent annually (unless they are circulating membership lists; see below)** although they should ask members to check their details annually to ensure their records are accurate. The final *italicised* point (*don't penalise individuals who withdraw consent)* may be impossible to meet given the need for a legal basis to hold members data. It should be borne in mind if a club's constitution is modified.

Withdrawal of consent

A clear process for withdrawal of consent should be defined and communicated to members (e.g. on the consent form and in a members' handbook or equivalent online members area).

Membership lists

The BMC raises the following issues with membership lists. It should be noted that the guidance merely states *"at appropriate intervals".* There seems to be no requirement for annual consent in either the UK ICO guidance or the EU article 29 working party guide. Clubs are advised to draw their own careful conclusions on this.

1. *For member details to be made available to other club members (in any format) the specific consent from each member will be needed.*

2. *Clubs must allow members to opt-in to what details are circulated and must allow members the option of not having any details circulated. It must not be a condition of membership of the club that details have to be shared.*

3. *Clubs will need to re-ascertain consent on a regular basis, ideally at least once a year.*

4. *Clubs need to be mindful that even though consent may have been given at one point it can be withdrawn at any future point, including the day after a club has posted out a club list to every member. If an individual withdraws their consent the club needs a clear way to action the withdrawal of that data. This could potentially result in a recall of all the club lists that have been posted out or the club may not*

be allowing the individual their lawful right of withdrawing consent. Because of this risk, clubs may decide that if they wish to use a club list then a secure area on the club website is easier to manage.

5. *Clubs need to ensure that data is accurate. If a member changes their contact details after the list has been produced clubs need to consider how the club will ensure that the club lists are updated, and that inaccurate data is not available to other members.*

6. *Clubs should consider what data needs to be circulated for communications between members, i.e. is a full postal address really needed in the 21st century, or is a phone number and/or email address more appropriate?*

7. *Clubs need to tell the recipients (members) what they can/can't do with the data in the lists, i.e. they can't pass or sell the data on to anyone else, and members can only use the data for club related communication.*

8. *Clubs need to ensure that data is not held for longer than is needed. A system would be needed by the club to ensure that club lists are deleted by members once superseded / not needed.*

Conclusion:

There appears to be two potential options for clubs when distributing membership lists to members:

a) They gain consent at least annually as advised by the BMC;
b) They gain consent less often (see
c) *Continued* Consent below) but **do not** send out addresses;

The BMC have taken this line because of the identifiability of address data and the principal of data minimisation. With email, mobile and home phone numbers members can contact each other if they need an address.

In essence: Either you must reduce the identifiability or ensure that your consent is still valid more often.

Continued Consent

Your continued consent will be sought at appropriate intervals; when there is a change to any of the following:

a) The law
b) How the club uses members data or the club's data protection policy.
c) The conditions of membership – e.g. an increase in the cost of membership subscription or BCA insurance.
d) Type of membership e.g. transfer from junior to probationary/adult/full membership at age 18.

The ICO guidance states that you should ***keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes***.

Section Four: Other Considerations

Under 18s Data

This can require the consent of a parent or guardian. If you use consent for the legal basis at aged 18 consent will be required from the individual.

Emergency contact details

This type of data is common on expeditions. It should be accurate, securely held with members aware of how to access this data only in an emergency. This should all be defined in a data protection policy.

Personal Data Breach

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority and the affected individuals.

- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

CCTV

While CCTV is data and covered by the GDPR; both UK and EU law impact on the use of CCTV and the need to register CCTV with the Information Commissioner's Office.

See: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Appendix A – Example Data Protection Statement

This example is from a club members handbook and uses legitimate interest as the lawful basis for the processing of data; the sharing of address, email, and phone numbers with other members of the club is by consent. **This is intended as an example only and may not work for all clubs or scenarios.**

Data Use Statement

ABOUT YOUR DATA: Only sufficient data will be sought and retained to administer the <INSERT CLUB NAME> and communicate with its members. The <INSERT CLUB NAME> holds and uses your data on the basis of legitimate interests.

Data is used for the following purposes:

a) The distribution of the club journal, newsletters and other paperwork, e.g. AGM notice.
b) The sharing of address, email, and phone numbers with other members of the club by consent.
c) Provision by <INSERT CLUB NAME> to the British Caving Association for their membership and administrative purposes. The BCA privacy notice http://www.british-caving.org.uk/privacy_notice sets out how <INSERT CLUB NAME> members data will be used by the BCA.
d) General club administration; e, g, collecting annual subscriptions, organising club events.
e) Administer visitors and members bookings to stay at the club hostel.

Your data will not be supplied to others or used for any other purposes without express consent of the member.

Data is held by the Secretary on <INSERT WHERE DATA IS HELD> and on the club website and shared with other Officers only to the extent required to fulfil their role. Only Club Officers as defined under <INSERT CLAUSE> of the constitution and the web hosting company contracted by The Committee may access the membership data.

You will be asked annually to check your details are correct and consent to sharing contact details (none, some or all from: i) address, ii) email, iii) mobile and iv) home number) with other members anywhere in the world. Where consented, members contacts details can be looked up in the members area of the club website, access to which is limited solely to other club members. The <INSERT CLUB NAME> Secretary will facilitate access for members unable or unwilling to use the club website.

If you do not want the Secretary to share your membership data with the BCA, then you must arrange your own insurance directly with the BCA. <INSERT CLUB NAME> requires all members to have membership of the British Caving Association for public liability reasons. You cannot be a member of <INSERT CLUB NAME> without BCA insurance.

Consent to share contact details data with other members

You will be asked if you want to consent to share your contact details with other members annually. ***You may withdraw or alter this consent at any time by contacting the Secretary.***

The membership details are held in a database behind the club website, accessible only to the Officers outlined above. Please use the website or contact the Secretary if you wish to amend your details.

If you do nothing, other members will not be able to view your contact details on the website and the Secretary will not give your details to other members apart from other committee members pursuing club business (uses a, c, d, and e in the previous section).

Right to Object

Individuals have the *right to object* to processing based on *legitimate interests.* ***You may exercise this right at any time by writing to the <INSERT CLUB NAME> Secretary to resign your membership.***

The Secretary will acknowledge this in writing, and remove your details removed from the club membership database, and in subsequent years the member will not be insured via the BCA. The letter will also request that the member cancel any standing orders they have with the club for paying membership subscriptions. The club is unable to cancel standing orders and cannot refund you as your contact details have been deleted! For this reason, a member's data will finally be destroyed in February of the year following their resignation.

Where a member has resigned under the right to object they can still be re-elected under <insert clause> of the constitution.

Appendix B - Example Legitimate Interests Assessment

<INSERT CLUB NAME>

Legitimate Interests Assessment (LIA).

This should be used alongside the Information Commissioner's Office legitimate interests guidance.

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

1. Why do you want to process the data? 2. What benefit do you expect to get from the processing? 3. Do any third parties benefit from the processing? 4. Are there any wider public benefits to the processing? 5. How important are the benefits that you have identified? 6. What would the impact be if you couldn't go ahead with the processing? 7. Are you complying with any specific data protection rules that apply to your processing (e.g. profiling requirements, or e-privacy legislation)? 8. Are you complying with other relevant laws? 9. Are you complying with industry guidelines or codes of practice? 10. Are there any other ethical issues with the processing?	
1	*The data needs to be processed to allow the club to function as a membership organisation. Personal data needs to be collected for:* *a) The distribution of the club journal, newsletters and other paperwork, e.g. AGM notice;* *b) The sharing of address, email and phone numbers with other members of the club by consent;* *c) Submission to the British Caving Association for their membership and administrative purposes. The BCA privacy notice http://www.british-caving.org.uk/privacy_notice sets out how <INSERT CLUB NAME> members data will be used by the BCA;* *d) General club administration; e, g, collecting annual membership subscriptions;* *e) Administer visitors and members bookings to stay at <enter name of hut>, the club hostel.*
2	*The member gains from the processing by being able to access the benefits of membership, and all members of the club benefit from the ability to go caving (and other related activities) as a group using shared resources (e.g. ropes, rigging equipment).*
3	*The BCA insurance scheme provided to all members of the how <INSERT CLUB NAME> indemnifies landowners against liability from granting access to their land to cave. This covers all cavers throughout the United Kingdom.*
4	*The BCA and its members benefit from the processing by being able to function as the national authority of an internationally recognised sport.* *A key benefit is the public liability insurance schema administered by the BCA on behalf of all members.* *The <INSERT CLUB NAME> is a member of the Council of Northern Caving Clubs and takes part in cave conservation to help maintain the underground environment for future generations.* *The club hostel is available for booking by others (mainly cavers) on a not for profit basis.*

5	*They are essential member benefits of belonging to the club and the BCA.*
6	*If we couldn't contact members, they would miss out on all the benefits of BCA membership as well as club membership. The BCA negotiates and administers a group insurance schema on behalf of all cavers; membership is a requirement for all club members.*
7	*Not applicable.*
8	*Yes.*
9	*Yes (British Mountaineering Council GDPR guidelines).*
10	*No.*

Assessment: this clearly shows a legitimate interest behind the processing

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

1. Will this processing actually help you achieve your purpose? 2. Is the processing proportionate to that purpose? *3.* Can you achieve the same purpose without the processing? 4. Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?	
1	*This processing is essential for the club and BCA to provide services to members.*
2	*Yes. No additional processing is carried out other than that required to service the needs of members.*
3	*No. You would become an individual caver with no shared resources*
4	*The processing is the minimum required for the purpose. We <u>do not</u>:* • *Circulate address lists to members; members are asked to consent to sharing contact details (none, some or all from: i) address, ii) email, iii) mobile and iv) home number) with other members anywhere in the world. Where consented, members contacts details can be looked up in the members area of the club website. The <INSERT CLUB NAME> Secretary will facilitate access for members unable or unwilling to use the club website.* • *Maintain a list of next of kin details or keep information on the medical conditions of members;* • *Require unneeded data (e.g. date of birth);* • *Engage in any sales or marketing activity.*

Assessment: the processing is necessary for the purpose identified.

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

The <INSERT CLUB NAME> did not meet any of the mandatory or optional requirements for a data protection impact assessment.

Nature of the personal data	
1. Is it special category data or criminal offence data? 2. Is it data which people are likely to consider particularly 'private'? 3. Are you processing children's data or data relating to other vulnerable people? 4. Is the data about people in their personal or professional capacity?	
1	*No.*
2	*Name and address: required for the delivery of club communications to members without email addresses (9%) and required by the BCA for the administration of the insurance scheme and to communicate to its members.*
3	*Yes. Parents/guardians must agree to membership and accompany their children at all times.*
4	*Personal.*
Reasonable expectations	
1. Do you have an existing relationship with the individual? 2. What's the nature of the relationship and how have you used data in the past? 3. Did you collect the data directly from the individual? What did you tell them at the time? 4. If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? 5. How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? 6. Is your intended purpose and method widely understood? 7. Are you intending to do anything new or innovative? 8. Do you have any evidence about expectations – e.g. from market research, focus groups or other forms of consultation? 9. Are there any other factors in the particular circumstances that mean they would or would not expect the processing?	
1	*Yes.*
2	*The club has existing since 19xx. Data has essentially been processed in the same way since at least 19xx).*
3	*Yes; members apply for membership; go through a probationary period and are elected full members at an annual general meeting of the club a 60% majority. Membership is not renewed annually; members can be elected life members after 25 years.*
4	*Not applicable. No third party data is processed except for hostel bookings by phone, email and post and this data is destroyed in accordance with standard data processing practice.*
5	*Data has been collected since its founding in 19xx.*

6	*Yes. The club has a constitution that clearly defines its purpose and is well understood by the membership. In addition, there is a members handbook*
7	*No.*
8	*All members are able to (and do) feedback their expectations at well attended annual general and meetings and monthly committee meetings. The expectations of members are formally minuted.*
9	*Members expect the club to process the data in this way as the club would be unable to function without it.*

Likely impact

1. What are the possible impacts of the processing on people?
2. Will individuals lose any control over the use of their personal data?
3. What is the likelihood and severity of any potential impact?
4. Are some people likely to object to the processing or find it intrusive?
5. Would you be happy to explain the processing to individuals?
6. Can you adopt any safeguards to minimise the impact?

1	*i. Accidental use of CC: instead of BCC: when sending of PDF newsletters (or any communications to club members by the Secretary or other members of the committee) would require consent (see Appendix A); this is because you have circulated a list of emails to most members of the club.* *ii. BCA insurance has the following impact on data subject rights;* *a. Individuals have the right to object to processing based on legitimate interests. BCA insurance is a requirement for membership in most caving clubs and clubs cannot give members the right to opt out from BCA insurance and the data processing this implies.* *b. If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected. Members cannot:* *i. Withdraw without some social or economic disadvantage;* *ii. opt out;* *iii. be anonymous.*
2	*No. They are invited to checks its accuracy on joining; annually and can resign (and therefore have their data deleted) at any time.*
3	*i. Disclosure of personal data outside of the defined scope of processing; this would normally require consent* *ii. Members would lose the benefits of <INSERT CLUB NAME> and possibly BCA membership (you can be an individual member of the BCA or hold membership through another caving club). The ability to book the hostel would be unaffected as long a sufficient non-member capacity is available on the requested dates.*
4	*No. Members are made fully aware of their right to object and to withdraw.*
5	*Yes. The club will continue to keep its members fully informed as to what processing it carries out.*
6	*i. A web-based email distribution system will be set up to ensure that communications to club members by the Secretary or other members of the committee cannot be accidentally CC:'ed to all members* *ii. Persons wishing to use the <INSERT CLUB NAME> club facilities but not wanting to disclose their personal information to the <INSERT CLUB NAME> (i.e. object, withdraw or opt out) may:* • *Book the hostel as a guest* • *Order journals and other publications from the Librarian if in print* • *Insure themselves directly as a BCA direct individual member* *The social or economic disadvantage of withdrawal is therefore minimised.*

Can you offer individuals an opt-out?	No

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing?	Yes
Do you have any comments to justify your answer? (optional) The <INSERT CLUB NAME> can use *Legitimate Interests* if combined with *consent* for children under 16 to provide a lawful basis for processing data.	
LIA completed by	
Date:	

What's next?

- Keep a record of this LIA and keep it under review.
- Do a DPIA if necessary.
- Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.