UNIVERSITY OF CAMBRIDGE
Sports Service

Data@Clubs & Societies

Guidance for GDPR and Data Security

2021-22 Edition

UNIVERSITY OF CAMBRIDGE SPORT

UNIVERSITY OF CAMBRIDGE
Sports Service

Contents

Section 1) Principles of the GDPR

The General Data Protection Regulation (GDPR) came into force on 25 May 2018 across the member states of the European Union[1]. This EU regulation supersedes domestic legislation and provides a series of rights and protections over personal data for natural living persons (i.e. individuals in their lifetime).

Here are some of the key definitions that appear in the GDPR and in this guidance:

Personal data

Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Consent

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

Many requirements of the GDPR extend those previously contained in the Data Protection Act 1998. In particular, the following principles should be observed by Clubs and Societies in relation to the collection and processing of personal data (which could, for example, be in the form of information provided on membership forms):

Principle	Explanation
1) Personal data should be processed **lawfully, fairly**, and in a **transparent manner**.	See section 2 for an explanation of the lawful bases that apply for data processing. Transparency involves being upfront and clear with members with how their data is collected and used.

[1] Note that it is expected for the effect of this regulation to remain in the United Kingdom after leaving the European Union.

2) The collection of personal data should be for a **specified, explicit**, and **legitimate purpose**, and not processed in a manner incompatible with that purpose.	This means that individuals must be made explicitly aware of the specific purpose of the collection of their data, and, once collected, the data is only processed in ways needed to achieve that purpose.
3) Data should be **adequate, relevant**, and **limited** to what is necessary in relation to the purposes for which they are processed.	This means that clubs should be precise with data collection; for example, it may be contrary to this principle to collect data on political views or sexual orientation if members are signing up to take part in activities to which political views or sexual orientation are of no relevance. Conversely, collecting relevant medical information may be important to achieve a safe response to any potential medical emergencies that may occur in the course of Club or Society activities.
4) Data must be **accurate** and kept **up to date**. Inaccurate data should be erased or rectified without delay.	For example, it is likely that alumni data, or data about longstanding members, may become out of date over time. Every reasonable step should be taken to ensure that inaccurate information is either updated, or erased.
5) The form of the data which permits identification of data subjects should be kept for **no longer than is necessary** for the purpose for which it is processed.	For example, once a member graduates and ceases to become an annual member of the club, there may no longer be a legitimate reason to hold their medical or emergency contact data.
6) Data should be **secured** and **protected** against unauthorised or unlawful processing and against accidental loss, destruction, or damage.	All personal information that your club holds should be processed securely. This may involve physically locking paper-based information away, and password protecting digital data. Robust procedures must also be in place to ensure that those with access to the data do not use or process it for unlawful purposes.

Overall, the approach of the GDPR is that information about individuals should be subject to privacy by default and design.

As a Club or Society, you are responsible for complying with these principles, and must be able to demonstrate compliance.

Section 2) Lawful Bases

For processing of personal data to be lawful, you need to identify specific grounds for the processing. This is called a 'lawful basis' for processing, and there are six options which depend on your purpose and your relationship with the individual.

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

Most lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason. If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).

Your Privacy Notice (see Section 5 and the Template in the Appendices) should include your lawful basis for processing as well as the purposes of the processing.

If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

The six options for 'lawful basis' are covered in more detail below. As previously stated, no single basis is 'better' or more important than the others but this document places greater focus on Consent, Contract and Legitimate Interests, as they are likely to be the most relevant to University Sports Clubs.

Consent

This is one of the three most relevant lawful bases to Clubs and Societies and applies where there is real choice open to members about whether or not they want their data to be processed in a certain way, if at all. Below are some best practice notes to follow for this basis:

1) Consent requests should be unambiguous; there must be a definitive **opt-in** for each processing operation. Therefore, a pre-ticked box or a box that requires an opt-out would generally not be compliant.
2) Generally, the consent you are requesting should **not** be a pre-condition for signing up to membership (i.e. there can't be an artificial choice).

3) Members must be able to withdraw consent after giving it; your club must have processes in place to ensure that this is actioned effectively.
4) If you can't offer a genuine choice to members, consent is not the appropriate lawful basis for data processing.
5) Consent requests must be prominent and not 'bundled in' with other terms and conditions of membership.
6) You must manage and update records of consent effectively.

Examples where the consent approach may be most appropriate:

- Sharing contact information with sponsors or partners.
- Using photographs of members for promotional purposes.
- Recording medical information to enable the club to respond adequately to potential injuries or illness.
- Managing and utilising your alumni records.

Contract

This basis can be relied upon if you process personal data in order to fulfil your contractual obligations to the data subject. When a member joins a Club or Society, most often a legal contract is formed – the member usually pays a membership fee, and in return, they may receive access to facilities, equipment, coaching, social events, etc. Part of this contract (even if a fee is not paid) may involve data processing necessary for the club to perform on these obligations, for example:

- Recording and sharing personal information to provide insurance to the member.

If the data processing is necessary for the performance of the contract, consent will not also be required. However, if **special categories of data** (see section 4) or **children** are involved, further explicit consent may be required. It's for this reason that health information cannot be processed under the contract basis, even though it would otherwise form part of the 'contract', and so instead consent is required.

Legitimate Interests

The 'legitimate interests' basis is likely to be appropriate when you use people's data in ways that they would reasonably expect; for example, using their email address to contact them with information about Club or Society activities or processing member data for statistical analysis. When using this basis, there should be minimal consequences for each individual's privacy.

- The basis is flexible, but would not necessarily be appropriate if consent or contractual bases apply.
- Extra responsibility is involved with this basis – the club must consider and protect people's rights and interests.
- A three stage test applies:
    - Are you pursuing a legitimate interest?
    - Is the processing necessary for that purpose?
    - Do the individual's interests override the legitimate interest?

- The member's right to object remains under this basis – i.e. they can ask you to stop processing their data in this way.
- The legitimate interests could be of a commercial nature, or interests of the data subject themselves (e.g. to receive information about Club or Society activities).
- **The Privacy Notice Template in the Appendices identifies Legitimate Interest as the legal basis, which is in line with the University's approach to alumni/supporter relations and fundraising.**

A consent or contract basis may apply first; however, some data processing will not fall under these options, and therefore the legitimate interest assessment may be an appropriate test.

Legal Obligation

This basis applies when the processing of data is necessary in order to comply with the law and will therefore be unlikely to be the legal basis used by University Sports Clubs.

Vital Interests

This basis applies when the processing of data is necessary to protect someone's life and will therefore be unlikely to be the legal basis used by University Sports Clubs.

Public Task

This basis applies when the processing of data is necessary or 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 and will therefore be unlikely to be the legal basis used by University Sports Clubs.

Section 3) Rights

The following rights must be protected under the GDPR:

1) The right to be **informed** about the collection and use of their personal data.

The purpose for processing personal data must be made transparent, and privacy information must be provided at the time the data is collected.

2) An individual's right to **access** their personal data.

*Reasonable information requests should be replied to promptly, and no later than **one month** after receipt. See the Subject Access Request Subsection below.*

3) Right to **rectification**.

Individuals have a right to have inaccurate personal data rectified. Rectification requests should be responded to within one month.

4) Right to **erasure**.

This is the 'right to be forgotten'. If an individual requests to be erased, clubs must respond within one month. There are various exceptions to this requirement.

5) Right to **restrict** processing.

This usually only applies if the individual wishes to challenge the accuracy of their personal data or if data has been unlawfully processed.

6) Right to **object**.

If there is processing based on legitimate interests, the individual has a right to object to this processing.

Subject Access Requests

The general method by which an individual exercises their right to access their personal data held by an organisation is called a Subject Access Request. Such requests can be made verbally or in writing and can request specific information or all information held by the organisation, including emails and all written communications.

It should be noted that responding to Subject Access Requests can be time-consuming and difficult. The guidance in this document will help your club to manage data effectively and ultimately limit the amount of data held such that Subject Access Requests would not be overly burdensome.

If your club receives a request, then they may contact the Sports Service Safety and Compliance Officer for guidance.

Section 4) Special Category Data

Additional protection arises for information about an individual's:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics
- Health
- Sex life
- Sexual orientation

Under Article 9 of the GDPR, processing of this information is forbidden unless the processor has both a lawful basis for the processing (see above) AND satisfies one of the Article 9 conditions. Some Clubs and Societies, may need to process health data (e.g. medical conditions that the Club or Society needs to be aware of to ensure

safe participation), and this information should only be processed with **explicit consent** for that specified purpose. In general, Clubs or Societies will not have any other need or lawful basis for collecting other special category data. However, there will be exceptions to this. For example, Clubs or Societies with political or religious affiliations or leanings may also need to process data regarding members' political opinions or religious or philosophical beliefs and will again need to obtain explicit consent for this purpose.

If in any doubt, Clubs and Societies should seek independent legal advice regarding their obligations under the GDPR before collecting special category personal data. Central University privacy notices exist, but these will not cover the local activities of your Club or Society's data processing. As such, Clubs and Societies are required to have their own privacy notice (also known as a 'Data Protection Statement', 'Data Management Statement' or 'Policy'). A template can be found at the end of this guide, but every Club and Society must ensure that their notice is accurate and specific to their own data collection and use.

Section 5) Club Privacy Notices

Because of the rights and obligations specified in the GDPR, as summarised above, your Privacy Notice should cover the following topics:

Topic	Example/Notes
1. The **purpose** of the personal data use.	*'We collect any relevant medical or injury information to ensure that your participation is as safe as possible.'*
2. The **lawful basis** for the personal data use.	This will almost always be via legitimate interest, contract or consent. *'We will use your personal information in accordance with the consents you have given to us.'*
3. Any **recipients** of shared data, if applicable.	*'We will share your email information with a third party email distribution software company for the purpose of sending you club mailings.'*
4. Where there is a **contractual** need to supply personal data, if applicable.	*'We need your contact details so that we can keep you informed of meeting and event times and locations.'*

5. How **long** data will be retained for.	*'We will retain your medical information for as long as you remain a paying and active member of the club.'*

This list is not exhaustive; if your club carries out data processing, you must ensure compliance with the principles and rights of the GDPR and be explicit and precise in your Privacy Notice.

Section 6) Retention Periods

When data is collected and processed for a certain purpose, the data should no longer be held or processed once that purpose ceases to exist.

In the context of University Clubs and Societies, it is unlikely that special category data or ancillary data needs to be retained once a member leaves, or ceases to take part in Club or Society activities. If a member consents to being kept in touch with after their contract with or membership of the club terminates, data processing must then be specific and proportionate to this purpose.

Section 7) Data Sharing

You should not publish or share the contact details of your members with third parties unless it has been clearly outlined to members in your Privacy Notice that you will do this.

Where you share personal data with a third party that processes that personal data on your behalf – such as a company that manages your mailings or cloud storage – you need to have a written agreement (e.g. a contract or a terms of service document) that outlines clearly the responsibilities of that company in handling personal data for you. The prescribed information that needs to be contained in this agreement is quite detailed. The ICO website provides a checklist to help.

If your Club or Society works with people or organisations overseas, personal data should not be transferred outside of the European Economic Area without your members' explicit consent (there are other lawful ways of transferring data abroad, but this is the most straightforward way to do this).

Section 8) Data Breaches

A serious breach of the GDPR can have significant consequences. Fines can be imposed of up to €20m or 4% of annual turnover, whichever is higher.

A breach may be a breach of security or an accidental loss, alteration, disclosure, or access to personal data (e.g. your membership database accidentally being published online). If a breach may pose a risk to people's rights and freedoms, there

is a duty to report the breach to the Information Commissioner's Office (ICO). If a breach is not deemed this serious, the breach must still be documented, and the non-reporting justified. You must report a notifiable breach without **undue delay**, and no later than **72 hours** after becoming aware of it.

While handling a breach is your responsibility, in the first instance you can contact the Junior Proctor's Office for further guidance.

Section 9) Security and Erasure

Data security can be maximised by putting in place proper procedures. Data can be stored in many mediums, including:

- Paper (e.g. membership forms and archives)
- Computer devices
- Online
- Electronic storage devices
- Film
- Honours boards and displays

It is important to audit all of your Club or Society's different mediums of data to ensure that each are processed correctly and protected from misuse.

Electronic Data

- Data stored online and on electronic devices can be more vulnerable to misuse because of the easy portability between devices and over networks. If your club does store member data in this way, it is important to take, as a minimum, the following steps:
    - Ensure that any online data is secured behind password protection and encryption (i.e. not open to the public).
- You may also need to verify the robustness of the service provider you are using to ensure protection against cyber-attacks, and the data protection laws of the countries in which the provider operates/locates its servers.
- Password protect any electronic devices that contain access to data. This includes mobile devices that may be linked to online data storage apps.
- Ensure that virus protection is up to date on electronic devices holding data.
- Verify that only authorised personnel have access to electronic data and restrict the ability of authorised personnel to give access to third parties.

Physical Format Data

Data stored on paper (e.g. membership forms) or other physically recorded means should be physically secured. This may be achieved by locking the information in a safe or cupboard, or, at the very least, storing it in a locked room with access limited to authorised personnel.

Erasure

One new aspect of the GDPR is the 'right to be forgotten'. If anyone you hold data on makes such a request, effective data erasure should be ensured. Destruction of physical copies may be possible via shredding, however electronic data may be more difficult to permanently remove. This is because of the possibility of copying data and multiple copies stored simultaneously. These problems not only emphasise the need for effective control and security of data when it is collected and processed, but also demand effective deletion procedures.

Expired Purpose

Remember that data processing is only permissible under the GDPR where there is a lawful basis and a purpose for doing so. If the purpose for holding or processing data 'expires', the data should be either deleted, or no longer processed.

One way of achieving effective controls over this is to specify **retention periods** for each of the data you collect. See Section 6 for an overview of the principles of data retention.

Section 10) Personal Data Audit

In order to practically support the rules outlined above, and to manage your Club or Society's collection and use of personal data effectively, you will need to assess and audit:

- **What** personal data you hold – you should not collect or keep more than you need.
- **Why** you hold personal data – this is likely be membership administration for all clubs, but may also extend to marketing and/or fundraising.
- **How** you use personal data – you should keep it accurate and you should not keep it for longer than you need.
- **Where** you store personal data – you should hold it securely, with access limited to those who need to see it (see section 8 for further guidance).
- **When** you might share personal data with third parties (i.e. any individual or organisation external to the Club or Society).

It is recommended that you produce a document auditing this information to maximise the Club or Society's effectiveness at compliance.

Further Information

This guidance is intended as a helpful overview of the law only and is not exhaustive. It does not constitute legal advice and Clubs and Societies are encouraged to check any statements contained herein to ensure they are accurate and up-to-date before relying on them, and to obtain independent legal advice regarding the Club or Society's particular circumstances as necessary. The University accepts no responsibility for non-compliance by Clubs and Societies with data protection law.

Some helpful resources can be found at:

ICO Guidance:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

University Guidance:

https://www.information-compliance.admin.cam.ac.uk/data-protection/guidance/societies

Appendix I – Sample Privacy Notice Statements

All clubs are required to have a privacy notice, and members must be provided with this at the point they join, and subsequently these must be readily available (e.g. on your website). A template statement is available at the end of this guide for clubs to adapt.

Below are examples of wording that can be used in sports club privacy notices covering:

a) The data you are collecting

b) The purpose of the collection and processing

c) The lawful basis of the processing

d) The duration of the processing and/or storage

Note that statements must be compatible with the principles and rights outlined above. Although the examples provided may be suitable for your club, each privacy notice must be bespoke and highly specific to the data processing of your club. These should therefore not be seen as compliant or relevant for every club or every processing activity.

Medical Information:

'We require your consent to collect information about any relevant medical or health issues which may impact your participation in sport. We use this information to ensure that the Club and its coaches can deliver a safe and appropriate program of training for our members. We will retain and process this information for as long as you remain an active playing member of the Club.'

Club Communications:

'In order to provide you with information, per your membership contract, we will use your contact information to send you emails about club activities and notifications. We will retain your contact information for as long as you wish to be contacted by the club, both in your capacity as a current member, and your future capacity as an alumnus.'

Third Party Marketing:

'We require your consent to share your contact information with third parties who may wish to send you relevant marketing information. We will share your information for as long as we have consent to do so, and no longer than the duration of your membership with the Club.' When you ask for consent for data processing, this lawful basis requires explicit and unambiguous means of obtaining it. The following example shows how this may be achieved for club social communications on a membership form.

Please note that any 'tick boxes' must not be pre-ticked, and consent should be **affirmative** – i.e. not an opt-out. If this option is required when a member fills out a membership form, it must be prominently placed on the membership form and not in the privacy policy (though the consent statement may appear in the privacy policy, as explained in Appendix I).

If you would like to receive club social communications, please opt-in by ticking the box below:

Opt-in to receiving club social communications: ☐

Appendix II – Sample Consent Request

Privacy Notice Template.

The University accepts no liability for this template which is provided as a guide. If you have complex arrangements relating to personal data (particularly in relation to non-members), you may wish to check the ICO guidance and/or seek independent legal advice to ensure your compliance with this aspect of the law.

Please note that that this template was developed by CUDAR so as to ensure that clubs can approach alumni relations and fundraising without concerns over data compliance. The template will require a significant degree of personalisation according to the circumstances within your club.

[text exclusive to fundraising in blue – delete if you do not conduct fundraising]
[lists highlighted in yellow should be amended, added to, or have items removed depending on your circumstances]
This statement explains how the [Alumni Group, Club, or Society] ("we" and "our") handles and uses the personal data we collect about our members and our past, current and future supporters ("you" and "your"). Developing a better understanding of our members and supporters allows us to keep in touch with you, in order to keep you apprised of our activities and developments, to provide services to you, and to identify ways in which you can support us, through donations or other forms of financial and non-financial support.
We are committed to protecting your personal information and being transparent about what information we hold.

Personal data that we hold

We may hold information relating to you from a number of sources. A significant proportion of the information we hold is that which you provide to us (for example, you may give us information by filling in forms on our website, or by corresponding with us by telephone, email or otherwise).
Most records contain:

- details of your education (e.g. your University, the courses you have completed, dates of study)
- unique personal identifiers and biographical information (e.g. student number, date of birth)
- your contact details (and we update these whenever you let us know that they have changed)
- details of your interactions with us, including:
    - your membership and achievements with us
    - your attendance at our events
    - other contact with us or our partners (as listed below)
    - details of benefits and services provided to you

    - your relationships with other members or supporters
- details about your family (e.g. your marital status, the name of your partner or spouse)
- personal data provided by you for a specific purpose (e.g. disability and dietary preferences for event management purposes)
- your communication preferences, to help us provide tailored and relevant communications

We also record, where applicable, based on information which you provide to us and, in some cases, publicly available information and information from our partners (as listed below):

- financial information relating to you and your family, including:
    - your history of donations made to us
    - your ability and willingness to make donations, including our assessment of your income and whether particular donations or funding appeals may be of interest to you
    - your philanthropy and other giving, including donations to other organisations and other support that you provide (e.g. details of volunteering roles)
- your career highlights and other life achievements
- information about your areas of interest and extra-curricular activities

We augment the data we hold with data from our partners (as listed below) and publicly available data.

We use targeted internet searches and may search the following websites (either directly or using search engines), where relevant in order to obtain and maintain the accuracy of the data listed above:

- Public sources for individuals:
    - Sunday Times Rich List
    - Other rich lists, including Forbes Magazine's international rich lists
    - Property websites
    - The Queen's Honours Lists
    - National change of address services
    - LinkedIn, to check business details
- Press sources, for negative press for due diligence purposes

How we use your data

Your data is used by us for a number of interdependent purposes in support of alumni relations, supporter communications and fundraising. These include:

- Maintaining your personal details (e.g. your name, photograph, membership number and preferred contact details), including ensuring effective communications with you.
- Keeping financial records (e.g. payment of your membership fees).
- Maintaining a formal record of your activities with us.

- Undertaking research into our activities.
- Managing complaints made to us.
- sending you publications (e.g. magazines and updates about our activities)
- conducting surveys, including research on when and whether particular donations or funding appeals may be of interest to you
- providing services
- sending you tailored proposals, appeals and requests for donations
- sending you details of volunteering opportunities
- inviting you to our events
- wealth analysis and research in order to improve our understanding of our members and supporters, inform our fundraising strategy and target our communications more effectively
- internal record keeping, including the management of any feedback or complaints
- administrative purposes (e.g. in order to process a donation you have made or to administer an event you have registered for or attended)

Before seeking or accepting major donations we are required to conduct due diligence, including reviewing publicly available personal data relating to the donor's criminal convictions and offences.

Communications to you may be sent by post, telephone or electronic means (principally by email), depending on the contact details we hold, the consent that you have provided, and the preferences expressed by you about the types of communications you wish to receive.

If you have concerns or queries about any of these purposes, or how we communicate with you, please contact us using the details listed below.

We may use automated or manual analyses to link data together to help us identify your potential for supporting us, to provide you with an improved experience, to send you communications which are relevant and timely, to identify volunteering opportunities or opportunities for providing support which may be of interest to you, and to avoid approaching you with opportunities which are not of interest. All of this enables us to raise more funds, sooner, and more cost-effectively, in support of our strategic objectives. We always seek to ensure that any opportunities we present are aligned with your interests, based on the research we conduct.

We will always respect a request by you to stop processing your personal data, and in addition your statutory rights are set out below.

When we share your data with others (our partners)

We share the above categories of data with the University and the Colleges to provide you with a coordinated approach and for specific purposes, such as for registration as a University Sports Club, to provide your blues and sporting records, or for supporter relations and fundraising. Any transmission of data to or from the University and Colleges is managed through agreed processes which comply with relevant data protection legislation. The University and each College has its own data protection statement and procedures.

We share some of your personal information with [name of third party] for the purposes of [insert details].

We use University IT facilities to store electronic copies of personal information.

We may share your personal information with certain organisations overseas, including [name of third party], as part of arrangements related to your membership of the club. In such cases, we will ask for your explicit consent prior to transmitting this information.

We share some of your personal information with [name of third party] for the purposes of [insert details].

We may share your personal information with certain organisations overseas, including [name of third party], as part of arrangements related to your membership of the society. In such cases, we will ask for your explicit consent prior to transmitting this information.

Additionally, we share the above categories of data on a considered and confidential basis, where appropriate, with:

- third parties engaged by us to provide fundraising related services, such as:
    - companies that provide us with data about alumni and supporters
    - consultants advising us on individuals' capacity to donate
    - other contractors providing services to you on our behalf or services to us
- selected companies who provide products and services that we endorse

How we protect your data

We ensure we have appropriate data sharing arrangements in place before sharing your personal data.

We do not sell your personal data to third parties under any circumstances.
We also facilitate communication between individual members, but in doing so we do not release personal contact details without prior permission.

Any transfers of your data overseas (outside of the European Economic Area), as set out above, are protected either by an 'adequacy decision' by the European Commission (declaring the recipient country as a 'safe' territory for personal data) or by standard contractual clauses adopted by the European Commission (which give obligations for the recipient to safeguard the data). Further information about the measures we use to protect data when being transferred internationally is available from us (via the contact details are set out below).

Your rights

You have the right to:

- ask us for access to, or rectification or erasure of your data
- restrict processing (pending correction or deletion)
- object to communications or direct marketing
- ask for the transfer of your data electronically to a third party (data portability)

You have the right to lodge a complaint with the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

The legal basis for processing your personal data for the interdependent purposes set out above is that it is necessary for the pursuit of our legitimate interests, in order for the society to run effectively and efficiently. We always handle your personal data securely and minimise its use, and there is no overriding prejudice to you by using your personal information for these purposes. In addition, there is no statutory or contractual requirement for you to provide us with any personal data.

The controller for your personal data is the [Alumni Group, Club, or Society], and we can be contacted at [email or postal address].

Please contact us if you have any concerns or questions about the above information or you wish to ask us not to process your personal data for particular purposes. Where you have specific requests relating to how we manage your data, we will endeavour to resolve these, but please note that there may be circumstances where we cannot comply with specific requests.

We will retain your data indefinitely in support of your lifelong relationship with us or until you request us to do otherwise. We will publish any changes we make to this data protection statement and notify you by other communication channels where appropriate.

Where you exercise your right to erasure, we will continue to maintain a core set of personal data (name, membership details, unique identification number and date of

birth) to ensure we do not contact you inadvertently in future. We may also need to retain some financial records about you for statutory purposes (e.g. Gift Aid, anti-fraud and accounting matters).