A close up of a sign

Description generated with very high confidence

Basketball England GDPR Toolkit

[Clubs, Associations, regions & Local leagues]

What is the purpose of this toolkit?

Basketball England has put together this toolkit to help clubs, associations, local leagues and regions in the following ways:

* to understand what the new data protection laws require
* to provide practical steps to achieve compliance
* to signpost to further resources to help achieve compliance.

This toolkit is divided into five sections:

1. Practical Steps
2. Data Governance
3. Collecting and using data
4. Data security
5. Other rights for individuals

This toolkit also provides practical examples of policies and procedures that a club, association or region will need to have in place. The ICO has a large amount of guidance

available on its website, which can be found here: [**https://ico.org.uk/for-organisations/**](https://ico.org.uk/for-organisations/).

This toolkit signposts to specific pieces of guidance where appropriate.

Data protection can be a complex area, and this toolkit is not intended to give every

answer to every scenario or question, and everyone using this guide should review

guidance on the ICO website. It is, however, a starting point.

It does not seek to give legal advice. Basketball England is not able to give specific legal advice to clubs, associations or other bodies.

What do you need to know?

Basketball clubs, associations and relevant bodies use individuals’ data in almost everything they do. This includes obtaining and using data about players, referees, administrators, other volunteers, employees and website users.

What is personal data?

Put simply, personal data is any information which relates to a living person. Most obviously, this can be an individual’s name, but it could be their address, email address, medical history or sporting history. It can be held in many places, such as membership databases, club spreadsheets, committee minutes, disciplinary judgments, member application forms and many more. Personal data may be held at a clubs/associations/local leagues premises, or on individuals’ own equipment at their homes.

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. There are special rules around when and how we can process this kind of data and extra procedures may need to be put in place to protect this data. Special category data that we may hold include:

* Race and ethnic origin
* Religion
* Health details (including medical records)

What are the new laws?

From 25 May 2018, all organisations in the UK will be subject to the General Data Protection Regulation (GDPR). This will be brought in by an act of Parliament in the UK. GDPR builds on existing data protection law to give individuals more rights in relation to their data, and places an increased onus on all organisations, whether commercial companies or not-for-profit organisations, to secure individuals’ data and use it only as necessary.

In simple terms, GDPR will help protect our players, members and clubs. GDPR will ensure that data is kept more secure, and that organisations only hold the data that they need to. It will also increase transparency as to how data is used.

Organisations holding personal data will need to give more information to people about what they do with those people’s data, why, and for how long. They must also keep the information secure.

In the UK, the data protection regime is monitored and enforced by the Information Commissioner’s Office (ICO).

A close up of a sign

Description generated with very high confidence

Practical steps to take now

We recommend that you read the whole of this toolkit, but this section summarises some practical steps you can take now to help with compliance. The ICO has produced a general document on steps an organisation can take, which can be found here: [**Preparing for GDPR – 12 Steps**](https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf).

This section is designed to complement this with some practical steps appropriate for basketball clubs, associations and local leagues:

1. Allocate a suitable person (or people) to deal with personal data within your club/association/local league. Ensure that they read this toolkit and any other guidance. You could consider sending a message to your membership to see if anyone has had to consider GDPR as part of their working life.
2. If you have not done so already, put data protection on the agenda for an upcoming committee meeting, and ensure that the right people attend.
3. Consider what personal data you hold within the club/association/local league, and how this data is used (which might be for general administrative, disciplinary or marketing purposes). Cross-check against the reasons why you obtained this data – do you need the data for these purposes? Are these the purposes which you told people about when you collected the data, or are you using the data for additional purposes? A template spreadsheet for recording this is set out in Appendix 4. Using this is not mandatory, but you may find it is useful.
4. Review the template privacy notice and any existing policies you have – what (if anything) do you need to add to these?
   1. Does the privacy notice cover all activities undertaken by the club/association/local league? If not, you will need to add the additional activities.
   2. Will the processes for dealing with data breaches match relevant responsibilities within the club/association/local league?
5. Review who in your organisation has access to records containing personal data and determine whether it is necessary for everyone who currently has access to retain it. Consider password protecting and/or encrypting documents which contain personal data.
6. Make relevant volunteers and staff aware of GDPR and their responsibilities through providing this toolkit or any additional materials, such as guidance from the ICO website.

A close up of a sign

Description generated with very high confidence

Data Governance

What to do

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your club/association/local league structure and governance arrangements.

How to do it

It is important that someone takes proper responsibility for privacy and data within the club/association/local league and, ideally, they would have some relevant experience. Consider sending a message to your membership to see if anyone has had to consider GDPR as part of their working life. We recommend that this person is a member of the main committee so that they will have visibility of how data is used throughout the organisation.

Some organisations are legally required to designate a formal Data Protection Officer and for this person’s contact details to be provided to the ICO. Others may choose to, and some law firms, or consultancies, can provide an outsourced service.

Whether or not you formally register a Data Protection Officer with the ICO, what is important is that there is at least one person in the club/association/local league tasked with understanding what data is used and why.

Where to find more information

The ICO has produced guidance on Data Protection Officers, which can be found here: [**https://ico.org.uk/for-organisations/guide-to-the-generaldata-protection-regulation-gdpr/accountability-and-governance/dataprotection-officers/**](https://ico.org.uk/for-organisations/guide-to-the-generaldata-protection-regulation-gdpr/accountability-and-governance/dataprotection-officers/)

Demonstrating compliance

One of the key areas of the new law is that an organisation will have to demonstrate that it is compliant. Consequently, there is a larger emphasis on record keeping.

What to do

You will need to keep records of:

* the name and contact details of the data controller
* the purposes of why you process data;
* how long you process data;
* a description of the categories of individuals whose data you hold
* a description of how data is shared with, or obtained from, third parties and any international data sharing that goes outside the EEA.

How to do it

Some of this information can be included in a privacy notice, which can be hosted on your website. A draft privacy notice is contained in Appendix 1. This is designed to cover the sorts of activities that a club/association/local league would usually undertake. If you use individuals’ data for other purposes, then you will need to expand this as necessary.

You will also need a record of processing, at least for the sensitive and regular data processing that you carry out. This is in effect an internal register that sets out how your organisation uses data. Guidance and templates for this record of processing can be found on the ICO website.

If you rely on certain legal grounds for processing sensitive data, like processing sensitive data for employment law purposes, you will also need a policy document setting out how you approach data protection principles, particularly retention and deletion.

You should also consider if any particular teams or people in your organisation need guidance on how to handle data, or requests for individuals.

You will need to produce this documentation if the ICO requests it.

Where to find more information

For guidance on the documentation required, and in particular if you have 250 employees or more, see here: [**https://ico.org.uk/for-organisations/guideto-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/**](https://ico.org.uk/for-organisations/guideto-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/)

Awareness and Training

What to do

It is good practice for all those people who collect or use personal data to receive training on this.

How to do it

We suggest that this toolkit is sent to all members of the committee of the club/association/local league, and any administrator or registrar.

Where to find more information

The ICO has a range of materials available, which can be found here: [**https://ico.org.uk/for-organisations/resources-and-support/**](https://ico.org.uk/for-organisations/resources-and-support/)

A close up of a sign

Description generated with very high confidence

Collecting & Using Data

A fundamental principle of the law is that an organisation must only use data fairly, lawfully and transparently. It must be clear to an individual how it uses his or her data, and why. This is usually set out in a privacy notice, which can be hosted on a website.

What to do

Any organisation must be clear on why it is collecting and using data and then only use it for those purposes. There are a number of lawful ways in which an organisation can use an individual’s data. Sometimes an individual must give consent for his or her data to be used, but in many cases consent is not actually necessary.

How to do it

You will need to ensure that the reasons for handling individuals’ data fall within one of the lawful grounds for processing set out in the GDPR and the new law which will enact it. The principal grounds are set out below. Note that this means that you will often have an alternative to seeking the individual’s consent for their data to be used.

**Legitimate interest**

An organisation will be able to use an individual’s data without consent if they can show it is in their – or a third party’s – legitimate interests, and this is not outweighed by the rights and interests of the individual. An assessment as to whether we have a legitimate interest will need to be undertaken. This will need to be documented and kept to demonstrate compliance if required.

The basic running of a club/association/local league, will rarely need consent. The following processes will not require an individual’s consent (but you will need to explain to individuals that you are carrying out this processing. This should be done through a privacy notice – see below):

* recording who officiates at matches
* maintaining lists of players, members, referees, parents of children at a club etc.
* providing an individual’s details to Basketball England or a league for regulatory or disciplinary purposes.

**Legal Obligation**

An organisation may process an individual’s data if there is a legal obligation to do so. For example, where you are required to maintain accounting records, or provide information to HMRC, this will be subject to a legal obligation.

**Performance of a contract**

In addition, an organisation may use an individual’s data where it is necessary for the purposes of performing a contract.

**Consent**

There are some circumstances when you will need consent. Email marketing is a good example of this - you need consent to sign an individual up to receive marketing or promotional material by email, either from the club/association/local league, or from its sponsors or partners,. This must be “clear, affirmative consent” – it must be opt in, separate from other documents and cannot be bundled with a service or other unrelated offer (for example, you cannot make entry into a competition conditional on giving consent to marketing). Where you need an individual’s consent, it is important that you record that this has been given. Please see Section Four, Data Security.

It may be that your general club/association/local league newsletters sent out digitally would contain some sponsor advertisements or links to websites. When a document ceases to be a legitimate update, and starts to be marketing, is a question of degree, but a useful rule of thumb is that if adverts are incidental to the newsletter, it is not a marketing communication.

Note that only those 13 years old or over can give consent for online services, like marketing – for those under 13, you will need parental consent.

More detail on direct marketing rules can be found on the ICO website:

[**https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf**](https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf)

You may also need consent if you collect sensitive data from players or other individuals, such as health data, religion, ethnicity, sexual life or orientation, trade union membership or criminal records data.

**Privacy Notices**

How you use an individual’s data should be set out in a privacy notice. Appendix 1 contains a draft privacy notice which is designed to cover most usual activity a club/association/local league undertakes. If you undertake other activities, you may need to add to this, or provide a separate notice.

This privacy notice must be available to anyone whose data you use. The most obvious place for this to be made available would be on the website of the club/association/local league. If you do not have a website, you can consider how else this may be distributed to members and third parties, such as by email once per season.

**Cookie Policies**

If your club/association/local league has a website, they will also need a policy setting out how that website uses cookies. These tend to be in standard form and will often be provided by the company that has produced your website.

Accurate Data

What to do

Another principle is that data must be accurate and kept up to date. The law requires that “every reasonable step” is taken to ensure that inaccurate data is erased or corrected.

How to do it

You should review the data you hold on a regular basis.

Where to find more information

More detail on this principle can be found here: [**https://ico.org.uk/for-organisations/guide-to-the-general-dataprotection-regulation-gdpr/principles/**](https://ico.org.uk/for-organisations/guide-to-the-general-dataprotection-regulation-gdpr/principles/)

Purpose Limitation

What to do

As set out above, individuals’ data can only be collected and used for specified and legitimate purposes. It must not be used further in a way that is incompatible with these purposes.

How to do it

Ensure that you have a process in place that does not allow individuals’ data to be used beyond what you have told individuals you will use their data for. For example, if you collect individuals’ data for general administrative purposes, you cannot automatically add them to a database of people who receive commercial mailings from sponsors.

You could, however, use the data for reasons which are compatible with your original purposes for processing. For example, if you have obtained data in order to administer and manage the team, it would be compatible to process the data for maintaining a record of a club’s results, even if this is not specifically described in a notice.

Where to find more information

The ICO has further details on this on its website, which can be found here:

[**https://ico.org.uk/fororganisations/guide-to-data-protection/principle-2-purposes/**](https://ico.org.uk/fororganisations/guide-to-data-protection/principle-2-purposes/)

Privacy by Design and Data Minimisation

What to do

Related to transparency, another principle of the law is that organisations must only hold and use the data that they actually need to use.

Even where there is a legitimate interest, or consent, for collecting and using data, you should ensure that you only collect the data that you actually need.

How to do it

When collecting data, consider why you are doing so, and what you need. Every piece of data you collect should be necessary for a purpose you have set out in your privacy notice. For example, only collect bank details if you actually need to use them. In particular, be careful only to collect sensitive data (such as ethnicity, health information, religion or sexuality) if this is absolutely necessary for a particular purpose. Always consider if you could use information at an anonymous level instead. It may be that you do need to collect health and medical information, for example from players. As set out above, this will need consent.

Where to find more information

For more information, please visit the ICO website.

Data Protection Impact Assessments

What to do

Where the club is using individuals’ data, there are some occasions when it must conduct a Data Protection Impact Assessment (DPIA). Most clubs are unlikely to need to carry out DPIAs as a matter of course, because they are required where new technologies are used and there is a high risk to the rights of individuals. DPIAs may be required, however, if a club has or installs CCTV on a large scale.

How to do it and where to find more information

Further details on when a DPIA must be carried out can be found here:

[**https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protectionimpact-assessments/**](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protectionimpact-assessments/)

Further guidance on how to carry out a DPIA can be found here:

[**https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf**](https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf)

The ICO has also produced a code of practice for CCTV, which can be found here:

[**https://ico.org.uk/media/for-organisations/documents/1542/cctv-codeof-practice.pdf**](https://ico.org.uk/media/for-organisations/documents/1542/cctv-codeof-practice.pdf)

Retention Periods

What to do

You will need to state the maximum time period for which you will retain individuals’ data. It may be that you need to retain data for a long time. You may keep some data indefinitely for historical and record purposes, such as match results and team lists. For other information, it will be appropriate only to keep data for a shorter period of time. For example, you will not need to keep bank details of former employees.

How to do it

It would be sensible to include retention periods within the privacy notice, but you must ensure that you actually follow the policy and delete data when you say you will.

It is acceptable to retain members’ details, for example, while they are members – it is not necessary to remove them and add the details afresh each year. Nevertheless, it is important to make regular checks, perhaps at the start of each season, to check whether it is still necessary to keep each individual’s data. Having all of this data in one place, will make this process easier.

Where to find more information

The ICO has produced guidance, which can be found here:

[**https://ico.org.uk/for-organisations/guide-todata-protection/principle-5-retention/**](https://ico.org.uk/for-organisations/guide-todata-protection/principle-5-retention/)

A close up of a sign

Description generated with very high confidence

Data security

Security controls

What to do

It will be vital for your club/association/local league to implement appropriate security controls for all data. Some of these controls can be technological ones, but many other controls are very practical.

How to do it

For ways in which you store data, there are a variety of steps that you can take:

* if data is secured on a computer, ensure that antivirus software is kept up to date
* any computer on which data is stored has appropriate password protection and is kept secure
* any hard copy documents containing individuals’ data are kept secure and locked away
* if there are any databases or spreadsheets containing large amounts of personal data, consider whether these should be password protected.

Also, be aware of how data is transferred:

* if you send out spreadsheets or lists of individuals’ data, consider whether you need to send these all out by email, and to each recipient
* where emails are sent out to large distribution lists and there is no need for others to reply to all, ensure recipients are bcc’d rather than cc’d to avoid disclosing others’ contact details.

Where to find more information

A basic guide to technology security is here:

[**https://ico.org.uk/media/for-organisations/documents/1575/it\_security\_practical\_guide.pdf**](https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf)**.**

It is aimed primarily at small businesses, but it is a useful starting point for all organisations.

Reporting data breaches

A data breach is, put simply, a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

There may be a number of ways this can happen, such as a lost laptop, a file sent to the wrong recipient or a hack. It need not be technological, a lost hard copy file will also be a data breach.

What to do

You will need to have in place a procedure to manage a data breach. This will need to include a decision whether to inform those individuals whose data may have been disclosed, or to inform the ICO.

The key thing to consider is that you should act quickly.

How to do it

The procedure need not be complex. In fact, the simpler it is, the better. A suggested procedure is contained in Appendix 2. Note that this is only a suggested starting point and not a formal process approved by the ICO – you should work out a process which is appropriate for your club/association/local league. Depending on the size and complexity of the club/association/local league, there may be additional elements or steps you will need to consider, including which people to notify.

Where to find more information

The ICO has detailed guidance on what constitutes a data breach and what to do. This can be found here:

[**https://ico.org.uk/for-organisations/guide-to-thegeneral-data-protection-regulation-gdpr/personal-databreaches**](https://ico.org.uk/for-organisations/guide-to-thegeneral-data-protection-regulation-gdpr/personal-databreaches)

**Using third party providers**

Many organisations will use third parties to process data for them. This could be another company hosting a website, or for larger and more complex clubs other actions such as mailing houses for larger scale mailouts, or other technological providers.

What to do

There will be limited occasions where you may be a joint controller of data with another organisation.

Where a third party is using data on your behalf and under your instructions, it is more likely that the third party will be a “data processor”. You will need to have a contract with that third party, and it will need to ensure that the third party will process data in accordance with the GDPR, including having appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data. The ICO intends to produce some model clauses that any organisation can use. These have not yet been published, and when they are, they will be available on the Information Commissioner’s Office website.

**How to do it**

Where you engage data processors, you can ensure that these clauses, or similar clauses are contained in any contract.

Where to find more information

For more information please contact the ICO or visit their website.

International Data transfers

It may be that a third party processing data on your behalf transfers data outside the European Economic Area (EEA). For example, data may be stored in a cloud based overseas. This is important, as many jurisdictions outside the EEA have less stringent protections for individuals’ data.

What to do

Where you engage a third party data processor, find out whether they will hold individuals’ data outside the EEA.

How to do it

If the third party will hold individuals’ data outside the EEA, then check that they can provide adequate protection for that data by signing up to EU Commission approved model contract clauses, demonstrating that they have authorised Processor Binding Corporate Rules, operate in a white-listed country, or can rely on a Privacy Shield certification if they are based in the United States.

Where to find more information

For more information please contact the ICO or visit their website.

A close up of a sign

Description generated with very high confidence

Other rights of individuals

Right of access

An individual may request a copy of all data held by you. This is not a new right, but from 25 May 2018 organisations are no longer able to charge a fee for this, and the information must be provided within 30 days. More information also needs to be provided about how that data has been used and shared.

What to do

This can be an onerous task, but it is an important one. You will need to have a process for providing this.

How to do it

Ensure that there is an individual responsible for managing this process. A suggested process is contained in Appendix 3. You will need to find all data held by the organisation on that individual. If all individuals’ data is held in one place, this will be easier. You may need to go through emails, databases and other places where individuals’ data is stored. If an individual requests data held by a club/association/local league, then it is the responsibility of that club/association/local league to supply this – requests should not be forwarded on to Basketball England.

If an individual requests his or her data, we recommend engaging with him or her fully. Often an individual will only want a specific set or piece of information. It may be helpful to find out if this is the case so that only that piece of information need be provided.

Where to find more information

This is a complex area, as there are exemptions to a requirement to provide information, and it may not be possible to provide an individuals’ data when it is intertwined with the data of another individual and it is not reasonable to disclose this data. There is extensive guidance on the ICO website, here:

[**https://ico.org.uk/for-organisations/guide-to-the-general-data-protectionregulation-gdpr/individual-rights/right-of-access/**](https://ico.org.uk/for-organisations/guide-to-the-general-data-protectionregulation-gdpr/individual-rights/right-of-access/)

Other rights

There are a number of other rights afforded to individuals. These include a right to rectification if data is incorrect, a right to erasure of data (the socalled “right to be forgotten”), a right to have data restricted (so it is not actively used), and a right to object to how data is used. There are also rights in relation to automated decision making and rights of “portability” in some circumstances. Not all of these will be relevant.

You should also be aware that some rights do not apply in a sporting context. For example, an individual cannot use the “right to be forgotten” to remove all of their data if they are playing or coaching (as from a governance perspective it is important that this data is kept correctly), or if they are in a disciplinary process (including anti-doping or safeguarding).

Further information can be found here:

[**https://ico.org.uk/for-organisations/guide-to-the-general-dataprotection-regulation-gdpr/individual-rights/**](https://ico.org.uk/for-organisations/guide-to-the-general-dataprotection-regulation-gdpr/individual-rights/)