DATA PROTECTION POLICY

AUTHOR - BTBC COMMITTEE

BEXLEY TIGERS BASKETBALL CLUB

1. Introduction

What is GDPR?

GDPR is a new law which expands the rights of individuals to control how their personal information is Processed, and places a range of new obligations on organisations to be more accountable for data protection. It supersedes the Data Protection Act 1998 and is applicable from 25 May 2018.

What is Personal Data?

Personal Data is any information related to a person ("**Data Subject**") that can be used to directly or indirectly identify the person. Personal Data can be factual (for example, a name, gender, contact details, location or date of birth or even online identifiers such as IP addresses and cookies) or an opinion about that person's actions or behaviour.

What is Processing?

Processing is any activity involving Personal Data, including collecting, storing, disclosing, deleting or just viewing Personal Data. GDPR protects all Personal Data we Process regardless of the media on which it is stored (whether on computers, other electronic devices or in the cloud, or made up of paper records).

1.1 The Bexley Tigers needs to collect and use Personal Data about the suppliers, contractors, players, fans and other individuals who we come into contact with in order to carry out our work. This Personal Data must be Processed lawfully in accordance with the General Data Protection Regulation ("GDPR").

1.2 This Policy sets out what we expect from all Bexley Tigers employees, contractors, consultants and freelancers ("Bexley Tigers Personnel") in order for us to comply with GDPR. We have provided additional practical guidance in the text boxes to assist you, but should you have any questions or concerns please contact a member of the Data Protection Team. Contact details are set out at the end of this Policy.

1.3 You must comply with this Policy when Processing Personal Data. We could be exposed to significant financial penalties for failure to comply with GDPR. Non-compliance may also be made public and this could cause significant damage to our reputation. Failure to comply with this Policy may result in disciplinary action or, in the case of consultants, contractors and freelancers, termination of your contractual relationship with us.

1.4 Complying with GDPR is everyone's responsibility. The Executive Leadership Team and department heads are responsible for developing, implementing and documenting appropriate practices which align with this Policy and for ensuring that all Bexley Tigers Personnel under their supervision (directly or indirectly) comply. Further guidance and support should be sought from the Data Protection Team where required.

1.5 The Board has overall responsibility for ensuring compliance with this Policy. The Director of Legal Services is responsible for overseeing this Policy and developing related policies, guidance and training.

1.6 This Policy (together with any related policies or guidance) should not be shared with third parties without prior authorisation from the Director of Legal Services.

1.7 You should contact the Data Protection Team (contact details at the end of this Policy) with any questions about the operation of this Policy or GDPR, or if you have any concerns that this Policy is not being followed.

We may make changes to this Policy from time to time but, if so, all Bexley Tigers employees will be notified of any material changes. It is your responsibility to ensure that consultants/contractors who report to you are provided with the latest version.

2. Data Protection Principles

2.1 We must adhere to certain principles when Processing Personal Data. Personal Data must:

- 2.1.1 be processed lawfully, fairly and in a transparent manner;
- 2.1.2 be collected only for specified, explicit and legitimate purposes;
- 2.1.3 be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed;
- 2.1.4 be accurate and kept up to date;
- 2.1.5 not be kept for longer than is necessary (see section 8); and
- 2.1.6 be Processed securely using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

What do I need to do?
In practice, this means that you must:

1. Have a good reason for collecting and using Personal Data.
2. Keep Personal Data to a minimum – don't collect more Personal Data than necessary for any specific purpose.

3. Tell the individuals why you are collecting their Personal Data (see section 6).
4. Only use Personal Data for purposes individuals would reasonably expect you to use it for.
5. Make sure you have a legal justification to use Personal Data (see section 3).
6. Carefully consider how long you will need to keep and/or whether you still need an individual's Personal Data. Delete it securely or anonymise it once it is no longer needed (see section 8).
7. Always make sure that Personal Data - including any devices which contain such information — are securely stored and only accessed by those people who have a business need to do so (see section 9).

When developing new projects/systems/processes you can consider and implement these requirements during the Privacy by Design and Data Protection Impact Assessment phases (see below) but you must also apply these principles to ongoing/existing activities.

2.2 A final principle is "accountability". We must be able to demonstrate compliance with the principles above. This Policy is one of the mechanisms by which we do that.

3. Lawful Processing

3.1 We must not Process Personal Data unless there is a legal justification to do so in each case. These include:

3.1.1 the Data Subject has given their consent ("Consent");

Be aware that obtaining Consent is not as straight forward as it sounds. A Data Subject only consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or a positive action to the Processing. This means that silence, pre-ticked boxes or inactivity are not sufficient. Consent must also be freely given (i.e. represent a genuine choice) and must be as easy to withdraw as to give. Further, in the case of children we may require parental/ guardian Consent. Consent is unlikely to be the relevant legal justification for most of our Processing activities (other than for direct marketing purposes). We must keep records of all Consents obtained to demonstrate compliance with GDPR.

Where Consent is the justification for Processing Sensitive Personal Data (see section 4.1), a very clear and specific statement of consent is required ("Explicit Consent").

3.1.2 the Processing is necessary for the performance of a contract that we have with the Data Subject; For example, where a Data Subject has submitted their Personal Data in order to attend a Bexley Tigers run event, such as PL Live,

we may Process their Personal Data for the purposes of fulfilling our obligations to supply the Data Subject with a ticket and other related information.

3.1.3 to pursue legitimate interests which do not override the interests or fundamental rights and freedoms of Data Subjects;
We rely on this ground for much of our Processing (for example we need to Process Personal Data about players to register them and record their playing activities). Reliance on this ground still requires careful consideration. Where we seek to rely on "legitimate interests", we need to conduct a Legitimate Interests Assessment (which includes a balancing test between our interests and those of the Data Subject) at the outset of the project, to ensure that we have considered the impact the particular Processing activity may have on Data Subjects. Legitimate Interests Assessments must be conducted under the guidance of the Data Protection Team. The purposes for which we Process Personal Data for legitimate interests also need to be set out in applicable Privacy Notices.

3.1.4 to protect the Data Subject's vital interests; or (in some cases)
3.1.5 to meet our legal compliance obligations.
What do I need to do?
You are not required to make an assessment as to what legal justification exists for any proposed new Processing activity as this will be determined by the Data Protection Team. You are, however, required to notify the Data Protection Team at the outset of any proposed new Processing activity. Be aware that we will breach GDPR if we do not have and/or cannot prove that we have a legal justification for any Processing activity.

4. Sensitive Personal Data

4.1 We should only process Sensitive Personal when absolutely necessary.
What is Sensitive Personal Data?

Sensitive Personal Data is Personal Data revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life and orientation, biometric or genetic data, and relating to criminal offences and convictions.

4.2 Always contact the Data Protection Team when you encounter or want to collect any Sensitive Personal Data. Take care as Sensitive Personal Data can sometimes be revealed by other information, for example, next of kin details disclosing sexual orientation.

4.3 You need to be particularly careful in relation to the Processing of Personal Data relating to children and high-profile individuals (like players).
Children are identified as "vulnerable individuals" deserving of "special protection" under GDPR and therefore Processing of Personal Data relating to children carries certain risks meaning further restrictions apply. If you are working with children or organising events where children will be participating you will likely be Processing the Personal Data of children. Please consult the Data Protection Team prior to any project involving children.

4.4 Even though not within the definition of "Sensitive Personal Data" you must also handle financial information such as bank details, credit card information, transactional records, salary and expenses payments with particular care. Most Data Subjects would consider financially related Personal Data to be sensitive and you should be aware that separate confidentially and regulatory requirements may also need to apply to them.

5. Privacy by Design and DPIA

Privacy by Design
5.1 “Privacy by design” is a concept introduced by GDPR that promotes privacy and data protection compliance from the start of all projects. When designing, introducing or revising any systems or processes which involve the Processing of Personal Data you must work with “DABS” (see box below) to assess what appropriate technical and organisational measures (such as Pseudonymisation) can be implemented to ensure compliance with the Data Protection principles.

What is DABS?

The Data and Business Systems Group (“DABS”) has been established to oversee the governance processes for systems and data across the Bexley Tigers. One function of DABS is to support Bexley Tigers Personnel to devise and implement efficient and secure procedures for data handling and advise on adherence to GDPR requirements.
You should consult DABS at the outset of any new data project.

What is Pseudonymisation?

Pseudonymisation is the replacing of information that identifies an individual with pseudonyms so that the person cannot be identified without the use of additional information.

Data Protection Impact Assessments (DPIAs)

5.2 Whilst Privacy by design applies to all new projects that Process Personal Data, where a new project:

5.2.1 involves Processing Personal Data; and
5.2.2 represent a high risk for Data Subjects (including systematic and large-scale Processing), the we require that a DPIA is conducted before implementation. The aim of a DPIA is to identify, reduce and manage the risks. DPIAs should be undertaken by the project lead and DABS working together. You must inform DABS of all new projects which involve the Processing of Personal Data so they can determine whether a formal DPIA is required. In any event, consulting DABS will ensure nothing is overlooked and will help us comply with our record keeping obligations (see section 7).

6. Use of Privacy Notices

6.1 We must tell all Data Subjects why we are collecting their Personal Data and what we are going to use it for. We provide this information to Data Subjects by means of a "Privacy Notice". The Legal team has prepared various Privacy Notices for use in different situations to ensure that the necessary level of information required is concise, transparent, intelligible, easily accessible, and in clear and plain language so that the Data Subject can easily understand it.

6.2 Our main Privacy Notices are the Player Privacy Policy, which covers Players and associated individuals, and the General Privacy Policy for all other individuals (e.g. website
visitors).

6.3 A Privacy Notice should not necessarily be restricted to a single document as the privacy information may be best presented in a range of ways. All of the information given to Data Subjects about how their Personal Data is processed, taken together, constitutes the privacy information. Therefore, you should try to ensure that you deal with Data Subjects as transparently as possible by ensuring they are fully informed of the ways in which we are using their Personal Data and providing them with the Privacy Notice at the time the Personal Data is collected from them.

6.4 Even where Personal Data has not been obtained from the Data Subject (for example, where we have collected it from a third party or publicly available source) we must include the type and source(s) of information in a Privacy Notice. We must provide this information:
6.4.1 within a reasonable period (maximum one month from collection); or
6.4.2 if it is used to communicate with the Data Subject, at the latest, when the first communication takes place; or

6.4.3 before it is disclosed to anyone else.
6.5 We do not need to provide such information where it proves impossible or would involve a disproportionate effort or is likely to render impossible or seriously impair the achievement of the objectives of that Processing. In any event, we must still take appropriate measures to protect Data Subjects' interests, including by making the Privacy Notice publicly available.

What do I need to do?

If you are concerned that you are collecting Personal Data and that the Data Subjects are unaware and/or have not been provided with an appropriate Privacy Notice or that these notification obligations raise practical difficulties, you should consult the Data Protection Team. When DABS is consulted in relation to new projects (see section 5.1) they can advise on how best to communicate Privacy Notices.

7. Record Keeping

7.1 In order to comply with GDPR, DABS maintains an accurate and up-to-date "Data Inventory" which provides a record of all Processing activities conducted by us or on our behalf.

7.2 The Data Inventory documents the legal basis for Processing for all such activities, details about all third parties which are Processing Personal Data on our behalf and a description of those Processing activities.

What do I need to do?

Although this Data Inventory is maintained by DABS, your assistance is required to ensure that it is accurate and up-to-date. If you are implementing a new project involving Personal Data or you are planning to use Personal Data within your department in a new way, you must communicate this to DABS so that the Data Inventory can be updated as necessary.

8. Retention of Personal Data

8.1 We have a legal obligation to ensure that Personal Data is kept for no longer than necessary for the purpose for which it was collected. This means that Personal Data should only be retained for as long as is necessary to meet our operational needs or otherwise to fulfil statutory or regulatory requirements (for example for tax purposes, or health and safety purposes) or to defend any claims or complaints brought against us.

8.2 Decisions relating to the retention, archiving, disposal or anonymisation of Personal Data we hold should be taken in accordance with our Retention Policy and any department specific policies that have been developed in line with it. This includes requiring third parties to delete such data where applicable.

What do I need to do?

Project Leads must use the Retention Policy to set out clear rules on when and how Personal Data which is collected for specific projects should be deleted, archived or anonymised (as appropriate). If you are unsure of how to comply with these rules you should speak to the Data Protection Team.

All Bexley Tigers Personnel need to take responsibility for disposing of documents and records for which they have responsibility in an appropriate manner, whether hard copy documents, electronic files or electronic media (e.g. USB devices or other electronic devices). Please see the Retention Policy for more guidance.

You are responsible for the Personal Data stored within your work email account and the Personal Data of general business contacts which you collect and store in the course of your duties. Proactive management of your emails is essential. It is particularly important that any emails (including email attachments) which contain Personal Data are deleted after they are no longer needed for business purposes. For example, if you communicated with a competition winner it is unlikely that you will need to retain this once the competition was successfully completed. Where there is particular sensitivity, such as with high profile individuals or children, where the data has been received in error, or due to the nature of the data itself, there is an extra need for ensuring timely deletion. If you are ever unsure of whether or not a particular document or record should be disposed of, please speak to the Data Protection Team.

9. Security

9.1 By law, we must take appropriate technical, physical and organisational measures to protect Personal Data from misuse or accidental, unlawful or unauthorised destruction, loss, alteration, disclosure, acquisition or access. We do this by operating in accordance with our Information Security Policy.

9.2 We regularly review and test our systems and processes to assess our continued ability to meet our obligation to keep Personal Data secure. You may be asked to provide assistance to the IT team so that this can be done effectively.

10. Reporting Personal Data Breaches

10.1 GDPR requires us to report any Personal Data Breach to the data protection authorities within 72 hours, and in certain instances, to the affected Data Subjects.

10.2 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Head of IT and the Director of Legal Services (including outside of office hours) who will comply with our Data Breach Policy. If you are unable for whatever reason to reach the Head of IT or the Director of Legal Services immediately email welfare@bexleytigers.co.uk. You should preserve all evidence relating to the potential Personal Data Breach and try to provide as many details as possible (including what has happened, how it happened, how many and which individuals it has affected, and the type of Personal Data involved).
Personal Data Breaches include any unauthorised access to or disclosure of any Personal Data within our control, any accidental loss or destruction of Personal Data and unauthorised or accidental alteration of Personal Data. Examples of incidents include:

- Accidentally posting, faxing or emailing Personal Data to the wrong person.
- Sending a marketing email to a group of recipients on cc, rather than bcc, thereby disclosing the email addresses to the entire group of people.
- Disclosing Personal Data over the phone to someone who is not authorised to receive it (including where reasonable steps have not been taken to verify the identity of that caller).
- Loss or theft of a company laptop, company mobile device or a personal device used for work purposes.
- Loss or theft of paperwork or a USB stick containing Personal Data.
- Accidentally deleting Personal Data from our IT systems where it cannot be recovered.

If you are aware of a Personal Data Breach, or think you have caused one, you must report it. A failure to report a breach will likely lead to more serious consequences than reporting the incident without delay.

Further information on how we should respond to a Personal Data Breach is set out in the Data Breach Policy which all Bexley Tigers Personnel are required to read and comply with.

10.3 The Data Protection Team maintains a log of all incidents in order to comply with GDPR.

You must report all incidents (however minor) so that (i) a complete record of incidents can be maintained, and (ii) incidents can be escalated where necessary.
It is vital that a record of all reported Personal Data Breaches and violations of this Policy is maintained to ensure that such issues are not overlooked or repeated once resolved. This will help ensure that lessons learned from previous incidents are addressed, recommendations are implemented, and the approach to data protection can be revised as required.

11. Sharing Personal Data

11.1 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. You may only share Personal Data with third parties if:

11.1.1 they have a need to know the information for the purposes of providing the contracted services;

11.1.2 the Data Subject knows that their Personal Data is going to be shared in such a way, either by Privacy Notice or Consent as appropriate; and

11.1.3 contractual arrangements including data protection provisions have been put in place.

What do I need to do?

Before instructing third party service providers (including consultants) you should have instructed the Legal team to put in place an appropriate contract. If the Legal team has any concerns with the service provider's ability to comply with GDPR they may require you (or the service provider) to provide additional information to ensure that they have adequate technical, physical and organisational measures in place to protect the Personal Data we will be providing to them. If you are unsure as to whether the service provider needs or should have access to certain data you should consult the Data Protection Team.

Sharing Personal Data with other organisations

11.2 In the course of our normal business activities we also share a large amount of Personal Data with other organisations for example, Basketball England and FIBA. We have put in place data sharing agreements with these organisations which sets out the types of Personal Data that we share, how we share it, and the reasons for sharing it.

However, this does not mean we can share any and all Personal Data freely and without careful consideration. If you are asked to provide Personal Data or receive Personal Data in a new way or you have any doubts as to whether that Personal Data needs to be or should have been shared then you should consult the Data Protection Team.
Sharing Personal Data with official authorities

11.3 We may in certain circumstances receive requests from other third parties for access to Personal Data that we hold. This might include requests from the likes of the Police, HMRC, the Department of Work and Pensions, the Health and Safety Executive or other authorities for legitimate purposes. If you receive any such request, you must notify the Data Protection Team as soon as possible and before disclosing any Personal Data.

Transferring Personal Data outside the EEA
11.4 GDPR restricts data transfers to countries outside the 28 countries in the EU, and Iceland, Liechenstein and Norway (the "EEA"). You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

11.5 We may only transfer Personal Data outside the EEA where the organisation receiving the personal data has provided adequate safeguards. The Data Subjects' rights must be enforceable, and effective legal remedies for Data Subjects must be available following the transfer. This is a technical area and you should consult with the Data Protection Team where there is any proposed transfer of Personal Data outside the EEA.

12. Rights of Data Subjects

12.1 Data Subjects have certain rights in relation to their Personal Data, including rights to:
Information and Access

12.1.1 obtain confirmation of whether their Personal Data is being Processed;
12.1.2 access their Personal Data (i.e. to request a copy);
12.1.3 be provided with certain information about the Processing; Erasure, Restriction or

Rectification
12.1.4 have their Personal Data rectified, deleted or blocked (as appropriate) if their Personal Data is incorrect, incomplete or is being unlawfully Processed, or where they have withdrawn their consent (if applicable);

Portability

12.1.5 in certain circumstances, to request that their Personal Data is provided in a usable form so that it may be transferred to a third party;
Right to object or to withdraw consent

12.1.6 in certain circumstances, a Data Subject may have the right to object to the Processing of his or her Personal Data; including an absolute right to object to the Processing of their Personal Data for direct marketing purposes; and

12.1.7 if processing of Personal Data is based on the consent of a Data Subject or related person, the Data Subject may withdraw his or her consent to such Processing at any time.

12.2 If a Data Subject makes a request relating to any of the rights listed above, we will consider each such request in accordance with GDPR and our Data Subject Response Policy.

What do I need to do?

All Bexley Tigers Personnel need to be aware of and understand that various Data Subject rights exist. Requests do not need to take any specific form, provided that they are made in writing. If you receive any request whether phrased as the exercise of a Data Subject right or not, you must escalate it to the Data Protection Team as soon as possible. You should not attempt to handle any requests yourself although you should expect to assist the Data Protection Team in providing a response where reasonably required.

Note: you should also be aware that certain requests may lead to the disclosure of any and all information about an individual held by the Bexley Tigers, including anything that you may write about that individual whether he/she is a business contact or colleague in emails or otherwise. You are reminded to exercise good judgement in your written communications which refer to other individuals.

13. Training

13.1 You will be provided with training to help you comply with this Policy and GDPR but you should speak to the Data Protection Team about additional training to help you comply if you think it is required.

14. Complaints Procedure

14.1 If a complaint in relation to the Processing of Personal Data is made, and such complaint is not satisfactorily resolved internally, we will cooperate with the appropriate data protection authorities. In the event that it is determined that we or one or more Bexley Tigers Personnel failed to comply with this Policy or GDPR, upon recommendation of the data protection authorities or Data Protection Team, we will take appropriate steps to address any adverse effects and to promote future compliance.

14.2 If you wish to make a complaint about our Processing practices or the handling of Personal Data by Bexley Tigers Personnel, you can do this by emailing complaint@bexleytigers.co.uk or speak to someone in the Bexley Tigers Customer Service Team or a member of the Management Board.

15. Contact

contact@bexleytigers.co.uk