UK General Data Protection Regulation (GDPR)

Created: August 2018
Effective date: August 2018
Revised by: Head of Digital and Head of Safeguarding and Governance
Last review date: February 2026
Next review date: February 2027

1. About this policy

1.1. This Policy is to help Bloomsbury Football Foundation ("we or us" or "the Foundation") deal with data protection matters internally. It applies to all employees, contractors, coaches, volunteers, trustees/Board members and anyone else who processes personal data on the Foundation's behalf. It covers personal data processed in connection with our football programmes (including weekly sessions, camps, academies, schools delivery and other targeted programmes), safeguarding activity, fundraising/donors, marketing/communications, and our online registration/parent portal and booking/payment systems.

1.2. We handle personal data about current, former, and on occasion prospective participants (predominantly children and young people aged 3-18) and their parents or guardians, as well as employees, volunteers, Board members, other Bloomsbury Football Foundation members, referees, coaches, managers, contractors, third parties, suppliers, donors and prospective donors, school and local authority and facility contacts, and any other individuals that we communicate with.

1.3. In your official capacity with the Foundation, you may process personal data on our behalf, and we will process personal data about you. We recognise the need to treat all personal data in an appropriate and lawful manner, in accordance with the Data Protection Act 2018 and GDPR.

1.4. Correct and lawful treatment of this data will maintain confidence in the Foundation and protect the rights of participants and any other individuals associated with the Foundation. This Policy sets out our data protection responsibilities and highlights the obligations of the Foundation, which means the obligations of our employees, committee, volunteers, members, and any other contractor or legal or natural individual or organisation acting for or on behalf of the Foundation.

1.5. You are obliged to comply with this policy when processing personal data on behalf of the Foundation, and this policy will help you to understand how to handle personal data.

1.6. The Foundation management will be responsible for ensuring compliance with this Policy. Any questions about this Policy or data protection concerns should be referred to the Head of Digital. Where the matter relates to safeguarding information, the Head of Digital will liaise with the Head of Safeguarding and Governance as appropriate.

1.7. We process employee, volunteer, participant, referee, coach, contractor, committee, supplier and third-party personal data in connection with our administration and internal management. Our purpose for holding this personal data includes to be able to contact relevant individuals on Foundation business includes, to organise and market events (including training sessions and participation of teams in matches and leagues), to manage policies and incidents relating to safeguarding, and to manage our employees.

1.8. For employees, contractors and volunteers, the legal basis upon which we process your personal data are as follows:

1.8.1. If you have a contract with us then your personal data is processed for the purposes of allowing us to perform that contract;

1.8.2. If you do not have a contract with us then we have a legitimate interest in processing your personal data for the day-to-day running of the Foundation, and to enable your participation in the Foundation's activities.

1.9. Key systems used to process/store personal data include Microsoft 365 (including OneDrive/SharePoint), our participant registration/CRM system (currently Salesforce), the FA/league systems used for fixtures/registration (including Whole Game System), and our website/online portal and payment

tools used for bookings and donations. The Head of Digital maintains a record of processing activities and an up-to-date list of suppliers/processors.

1.10. The length of time that we hold this data for depends on the individual in question's involvement with us. For employees and volunteers, we retain your personal data for no longer than 12 months after the end of your official relationship with the Foundation, unless required otherwise by law and / or regulatory requirements. Guidance on retention policies for other participants' personal data is set out in our Privacy Notice.

1.11. If you do not provide your personal data for this purpose, you will not be able to carry out your role and/or the obligations of your contract (if applicable) with the Foundation.

1.12. All the key definitions under GDPR can be found here. Please ensure that you are familiar with those definitions.

2. What we need from you

2.1. To assist with our compliance with GDPR we will need you to comply with the terms of this Policy. We have set out the key guidance in this section but please do read the full Policy carefully.

2.2. Please help us to comply with the data protection principles (set out briefly in section 3 of this Policy and in further detail below):

2.2.1. Ensure that you only process data in accordance with our Privacy Notice;

2.2.2. Only process personal data for the purposes for which we have collected it (i.e. if you want to do something different with it then please speak to our Head of Digital first);

2.2.3. Do not ask for further information about players and / or participants and / or staff and / or volunteers without first checking with our Head of Digital;

2.2.4. If you are asked to correct an individual's personal data, make sure that you can identify that individual and, where you have been able to identify them, make the relevant updates on our records and systems;

2.2.5. Comply with our retention periods listed in our Privacy Notice and summarised below, and make sure that if you still have information which falls outside of those dates, you delete it or destroy it securely;

2.2.6. Treat all personal data as confidential. If it is stored in electronic format then ensure that the documents themselves are password protected and that your personal computer is password protected and consider whether you can limit the number of people who have access to the information. You should also consider the security levels of any cloud storage provider (and see below). If personal data is stored in hard copy format then make sure it is locked away safely and is not kept in a car overnight or disposed of in a public place;

2.2.7. If you are looking at using a new electronic system for the storage of information, talk to our Head of Digital first so that we can decide whether such a system is appropriately secure and complies with GDPR;

2.2.8. If you are planning on sharing personal data with anybody new or with a party outside the FA structure or local authority, then speak to our Head of Digital before doing so. They will be able to check that the correct contractual provisions are in place and that we have a lawful basis to share the information;

2.2.9. If you receive a request from an individual regarding their personal data (or think somebody is making such a request) then tell our Head of Digital as soon as possible because we have strict timelines in which to comply. Further details on rights that individuals may exercise in connection with the personal data that we may hold relating to them are set out section 13.

2.2.10. If you think there has been a data breach (for example, you have lost personal data or a personal device which contains personal data or you have been informed that another staff member has done so, or you have sent an email and open copied all contacts in) then speak to our Head of Digital who will be able to help you to respond. Further details are set out in section 14.

If you have any questions at any time, please ask our Head of Digital. We are here to help.

3. Data protection principles

3.1. Anyone processing personal data must comply with the following key principles. Personal data must be:

3.1.1. Processed lawfully, fairly and in a transparent manner (see sections 4 and 5 below);

3.1.2. Collected for only specified, explicit and legitimate purposes (see section 6 below);

3.1.3. Adequate, relevant and limited to what is necessary for the purpose(s) for which it is processed (see section 7 below);

3.1.4. Accurate and, where necessary, kept up-to-date (see section 8 below);

3.1.5. Kept in a form which permits identification of individuals for no longer than is necessary for the purpose(s) for which it is processed (see our Privacy Notice); and

3.1.6. Processed in a manner that ensures its security by appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (see section 10 below).

3.2. We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

4. Fair and lawful processing

4.1. This Policy aims to ensure that our data processing is done fairly and without adversely affecting the rights of the individual.

4.2. Lawful processing means data must be processed on one of the legal bases set out in the GDPR. When special category personal data (for example, data concerning health and medical history or racial and ethnic background) is being processed, additional conditions must be met.

4.3. Our Privacy Notice sets out the lawful bases on which we process data of individuals who participate in the Foundation's activities. Below we identify

the lawful bases that we rely on and where they apply. We also set out special considerations which apply to photos and videos.

4.4. **Legitimate interests:** Personal data is generally processed by us because it is in our legitimate interests to process such data for the proper administration and management of the Foundation and is necessary for the Foundation to provide its services. Such processing is not detrimental to the privacy rights and freedoms of individuals who participate in the Foundation's activities.

4.5. **Legal obligation.** We may process personal data where necessary to comply with legal/regulatory obligations (for example employment, tax, safeguarding and charity governance requirements).

4.6. **Vital Interests.** In rare cases we may process personal data (including health information) where necessary to protect someone's life, for example in a medical emergency at a session).

4.7. **Racial Origin/Ethnicity:** We process data concerning racial origin and ethnicity to ensure equality of opportunity and treatment. In addition, we are required to collect such data for the purposes of certain Local Authority funding. Where data of this nature is shared with the Local Authority for that purpose, it is anonymised.

4.8. **Special category personal data (including health and disability information):** We may process limited special category data where necessary to protect participants' health, wellbeing and welfare and for safeguarding purposes. We will identify and document an appropriate Article 9 condition for this processing (for example explicit consent in many routine cases, and/or a safeguarding/substantial public interest condition where that is more appropriate).

4.9. **Consent**: Where we rely on consent:

4.9.1. An individual consents to us processing certain data if they clearly indicate explicit, specific and informed agreement, whether in writing or orally.

4.9.2. Individuals must be easily able to withdraw their consent at any time and withdrawal must be promptly honoured.

4.9.3. Where consent is our legal basis for processing, it is obtained at the point in which a participant registers with the Foundation. Where consent is withdrawn then a record of that withdrawal and how it was given should be made.

4.9.4. Where the data in question relates to a child who is under 13 years of age, then the consent of the parent or guardian of that child must be obtained.

4.10. **Photos and videos**: You should not take photos or videos at Foundation-organised events, or at matches or tournaments for personal use. You may be asked to take photographs or videos of Foundation-organised events, or at matches or tournaments, for Foundation community and promotional purposes. In that case, the following rules apply:

4.10.1. Participants' parents or guardians, where under 18, will be asked when they register for Foundation activities if they consent to photographs or videos of them being published in line with our Privacy Notice. A clear opt-out process must be followed at sessions/events (e.g., the use of wristbands or coloured bibs) and photographers/videographers must check and respect that their photograph/video should not be published. Any request to withdraw image consent must be actioned promptly and referred to the Head of Safeguarding and Governance in line with our Privacy Notice.

4.10.2. If photos or videos of participants in Foundation activities are stored on your personal phone then it is essential that your phone is password protected. You must regularly delete photos or videos of participants from your personal phone, saving those that may be used for promotional purposes on the Foundation's Microsoft 365 drive.

5. Transparency

5.1. Our Privacy Notice provides details to individuals who participate in the Foundation's activities on how we may process their data, the lawful bases upon which we do so, circumstances in which their data may be shared, their rights in respect of their personal data, and applicable security measures.

5.2. Our Privacy Notice is reviewed annually and is published on the Foundation's website.

5.3. All employees, contractors and volunteers should ensure that they are familiar with the most up to date version of the Foundation's Privacy Notice.

6. Processing for limited purposes

6.1. We will only process personal data for the purposes of the Foundation. The purposes for which we collect different categories of personal data are set out in our Privacy Notice.

7. Adequate, relevant and non-excessive processing

7.1. We will only collect personal data that is required for the specific purpose notified to the individual.

7.2. You may only process personal data collected for us or on our behalf if required to do so in your official capacity with the Foundation. You cannot process such personal data for any reason unrelated to your duties.

7.3. When personal data is no longer needed for specified purposes, it should be deleted or anonymised. Further details are set out in our Privacy Notice and at section 9 below.

8. Accurate data

8.1. We aim to ensure that personal data we hold is accurate and kept up to date and if notified of any inaccuracies will correct the personal data that is held.

8.2. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

9. Timely processing

9.1. We will not keep personal data longer than is necessary for the purpose(s) for which they were collected. Retention periods differ depending on the purpose and legal/regulatory requirements. Where an individual stops participating, we will review their record and either delete/anonymise it or place it into an archived status, in line with the retention schedule in our Privacy Notice and internal retention rules. We reserve the right to delete data and remove accounts where it has been 3 years since the User's last log in (including longer retention for safeguarding/incident, finance and employment

records) or if the User has not held an active subscription for over 6 months or more.

9.2. If you have been asked to take videos or photographs of participants at matches or events, then it is best practice to immediately move the photos from any personal device to the Microsoft 365 drive and delete such photographs or videos from your phone once this has happened.

9.3. We may need to retain personal data for longer. If you have any questions on whether personal data should be retained, please contact the Head of Digital.

10. Data security

10.1. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

10.2. We have proportionate procedures and technology (including those set out below at paragraph 10.4) designed to maintain the security of all personal data.

10.3. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data.

10.4. Our security procedures include:

10.4.1. **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

10.4.2. **Secure desks, cabinets and cupboards.** Desks and cupboards should be locked if they hold personal data.

10.4.3. **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed.

10.4.4. **Equipment.** Screens and monitors must not show personal data to passers-by, and should be locked when unattended.

10.4.5. **Microsoft 365 accounts.** Individuals responsible for the day-to-day running of the Foundation's activities use Microsoft 365 accounts with multi-factor authentication.

10.4.6. **Access Controls.** Access to participant/safeguarding/finance data must be granted on a least-privilege basis and reviewed periodically.

10.4.7. **Sharing.** Personal data must be shared by link with appropriate permissions (not email attachments) unless strictly necessary, and never by open-access links.

10.4.8. **Emailing.** Use BCC where appropriate; do not 'open copy' distribution lists containing personal emails.

10.4.9. **Centralised Filing System**. Where participant data is exported it must be saved to our centralised filing system (OneDrive) which is password protected. If an exported file has to be shared (for the purposes of Foundation events or participation in matches or leagues) then a link to the file should be shared.

10.4.10. **Personal Devices.** Anyone accessing or processing the Foundation's personal data on their own device, must have and operate a password only access or similar lock function, and should have appropriate anti-virus protection. These devices must have the Foundation's personal data removed prior to being replaced by a new device or prior to such individual ceasing to work with or support the Foundation. You should not download or locally save Foundation files to or on personal devices.

10.5. Where personal data is held in our CRM/registration system, exports should be minimised, justified, and promptly deleted once no longer needed.

10.6. As set out above at section 2.2.7, if you are looking at using a new electronic system for the storage of information, talk to our Head of Digital first so that we can decide whether such a system is appropriately secure and complies with GDPR.

11. Disclosure and sharing of personal information

11.1. We share personal data of certain participants with organisations (such as The FA), and with applicable leagues using Whole Game System. Further details are set out in our Privacy Notice.

11.2. Where participants are involved in matches, tournaments, or other events then we may share certain of their personal data with the organisations responsible for those events.

11.3. We may share certain personal data (such as names on team sheets) with referees, coaches or match organisers.

11.4. Where we deliver sessions in schools or partner venues, we may share limited participant information with the school/venue where necessary for safe delivery (e.g., attendance lists, emergency contact needs).

11.5. Where required by funders/Local Authorities, we may share monitoring/reporting information (normally anonymised/aggregated).

11.6. Where safeguarding concerns arise, we may share relevant information with statutory agencies and/or other safeguarding partners where necessary and lawful.

11.7. Where we engage a third party to process data on our behalf (a data processor), we may share personal data with them. Personal data will only be transferred to that party where we have a GDPR-compliant written contract in place with that data processor.

11.8. We may also be under a duty to disclose or share an individual's personal data in order to comply with any legal obligation; in order to enforce or apply any contract with the individual or other agreements; or to protect our rights, property, or safety of our employees, participants, other individuals associated with the Foundation or third parties.

12. Transferring personal data to a country outside the UK and/or EEA

12.1. We may from time to time use cloud-based suppliers that may involve data being stored and/or processed outside of the UK or EU. Where international transfers occur, we will ensure an appropriate safeguard is in place. We use reputable service providers who provide appropriate protection in relation to data.

13. Dealing with Data Subject's Requests

13.1. As data subjects, all individuals have the right to:

13.1.1. Be informed of what personal data is being processed;

13.1.2. Request access to any data held about them by a data controller;

13.1.3. Object to processing of their data for direct-marketing purposes (including profiling which means any form of automated processing of personal data consisting of the use of such data to evaluate personal aspects of a person, including work performance, economic situation, health, personal preferences and interests, behaviour, and location and movement);

13.1.4. Ask to have inaccurate or incomplete data rectified;

13.1.5. Be forgotten (deletion or removal of personal data);

13.1.6. Restrict processing of their personal data;

13.1.7. Request their data be transferred to another person; and

13.1.8. Not be subject to a decision which is based on automated processing.

13.2. It is our policy to respect these rights. Any request from an individual to exercise their data protection rights must be forwarded immediately to the Head of Digital. We will verify identity where necessary, log the request, and respond within the required statutory timeframe (normally one month, subject to permitted extensions). We may seek external guidance where appropriate (including from the FA/County FA on FA-system data), but responsibility for responding rests with the Foundation.

13.3. Where the request relates to data held within FA systems (e.g., Whole Game System), we will explain what we can do and what the individual may need to request directly from the FA.

13.4. When receiving telephone enquiries, we will only disclose personal data if we are satisfied as to the caller's identity and their right to receive the data. An example would be asking the caller to identify their date of birth or postcode.

14. Reporting a personal data breach

14.1. In the case of a breach of personal data, we may need to notify the data protection regulatory body and the individual.

14.2. If you know or suspect that a personal data breach has occurred, inform the Head of Digital **immediately**, who may need to escalate to an external organisation as appropriate. You should preserve all evidence relating to a potential personal data breach.

14.3. The Head of Digital will assess any suspected breach promptly, contain it, and determine whether notification is required to the ICO (generally within 72 hours where the breach is likely to result in a risk to individuals) and/or to affected individuals (where there is a high risk). All breaches and near-misses must be recorded in a breach log, including the decision on notification.

15. Changes to this policy

15.1. We reserve the right to change this policy at any time. Where appropriate, we will notify you by email.

16. Further advice on GDPR can be obtained from:

Head of Digital: Richard Basteed
T: 07514 724237
E: r.basteed@bloomsburyfootball.com

Richard Basteed
Richard Basteed (Mar 11, 2026, 12:55pm)
Richard Basteed
Head of Digital

11 Mar 2026
Date

Charlie Hyman
Charlie Hyman (Mar 11, 2026, 9:17pm)
Charlie Hyman
CEO

11 Mar 2026
Date

*The procedure to review this document includes (1) the Head of Digital and CEO are to update the document annually; (2) appropriate advice will be sought to ensure the policies and procedures contained in the document comply with the relevant legislation and regulations; and (3) the Head of Digital and CEO will review the changes made to the document and sign it off when concluded.