GILLINGHAM FC
FOUNDATION

Data Protection Policy

1.0 Purpose

The Data Protection Policy ("Policy") sets out how the Gillingham FC Foundation, (we", "our", "us", "the Foundation") handle the Personal Data of our clients, suppliers, employees, workers, partners and other third parties. This Data Protection Policy ("Policy") sets out how the Foundation, ("we", "our", "us", "the Foundation") handle the Personal Data of our clients, suppliers, employees, workers, partners and other third parties.

This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, volunteers, beneficiaries, participants, donors, partners, suppliers, website users or any other Data Subject.

This Policy applies to all Company Personnel ("you", "your"). The sections of this Policy which are most relevant to you will depend on your role within the Foundation and how regularly you Process Personal Data. However, it is important that you read, understand and comply with this Policy, because it sets out how both you and the Foundation must Process Personal Data in order for us to comply with applicable law.

Your compliance with this Policy is mandatory and we are committed to increasing your awareness of compliant data protection practices. We may from time to time develop and circulate supplemental policies and guidelines to help you interpret this Policy.

It is important that you comply with all such supplemental policies and guidelines. Serious breaches of this Policy may result in disciplinary action. Once you have read and understood this Policy, please confirm that you have done so to your Line Manager through your Induction training and refresher training programme.

This Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from your Line Manager.

2.0 Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations.

Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Foundation is exposed to potential fines depending on the breach, for failure to comply with the provisions of the GDPR.

The Data Protection Officer (DPO) and heads of department are responsible for ensuring all Company Personnel comply with this Policy and developing any related policies and guidelines.

Please contact the DPO with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(i) if you are unsure about the retention period for the Personal Data being Processed;
(ii) if there has been a Personal Data Breach (section 8.7 below); and
(iii) if you need any assistance dealing with any rights invoked by a Data Subject (see section 9).

2.1 Personal protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(i) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
(ii) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
(iii) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
(iv) Accurate and where necessary kept up to date (Accuracy).
(v) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
(vi) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
(vii) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
(viii) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

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

3.0 Lawfulness, fairness and transparency

3.1 Lawfulness and fairness

(i) You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes.

(ii) The GDPR allows Processing for specific purposes, some of which are set out below:

- the Data Subject has given his or her Consent;
- the Processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests; or
- to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

(iii) The DPO will identify and document the legal ground being relied on for our Processing activities.

3.2 Consent

(i) A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient.

(ii) Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured.

(iii) Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, we must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

(iv) We will need to evidence Consent captured and keep records of all Consents so that we can demonstrate compliance with Consent requirements and we will require your assistance in doing so. Where you are relying on Consent as the legal basis for processing Data, please keep a record of when such Consent was obtained and the method by which it was obtained.

3.3 Transparency (notifying data subjects)

(i) The GDPR requires us to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, accessible, and in clear and plain language so that a Data Subject can easily understand them.

(ii) Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller, how and why we will use, Process, disclose, protect and retain that Personal Data through a Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data.

(iii) When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

4.0 Purpose limitation

(i) Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

(ii) It is important that you do not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

5.0 Data minimisation

5.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it and it Is important that you do not Process Personal Data for any reason unrelated to your job duties.

It is important that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the attached Data Retention Schedule and the Employee Data Retention Policy attached to the Fair Processing Notice circulated to all Company Personnel (together the "Retention Policies").

If you maintain any types of records that are not listed in the Retention Policies, and it is not clear from the existing record types in the Retention Policies what retention period should apply, please contact your head of department, the DPO for guidance.

6.0 Accuracy

6.1 It is important that we ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. Where possible, please check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Heads of department should advise team members how often the accuracy of data sets should be tested.

6.2 You should notify us if your personal details change or if you become aware of any inaccuracies in the data we hold about you or third parties.

7.0 Storage limitation

7.1 Please ensure you are not keeping Personal Data for longer than specified in the Retention Policy, which forms part of the Record of Processing Activities.

7.2 Please take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with the Retention Policies and all other applicable policies.

8.0 Security, integrity and confidentiality

8.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

It is important that you help us implement such measures and you should exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access. In order to do so, the following are deemed to be good practice.

8.2 Sending documents

(i) When sending documents that contain Sensitive Personal Data by e-mail, password protect the document before sending and communicate the password to the receiver by alternative means (eg. telephone or letter). Always double-check the recipient's e-mail address is correct to avoid accidental disclosure to other parties.

(ii) When sending documents that contain Sensitive Personal Data by post, please ensure the envelope or packaging is well sealed and mark the front with "Strictly private and confidential".

8.3 Security measures for electronic records

(i) We shall ensure that all the Foundation's devices have adequate protection against malicious software and/or viruses. Please do not install software onto the Foundation's devices without such software first being checked for viruses by the IT department.

(ii) All devices and electronic documents containing Personal Data should be password protected. The IT department will issue you with passwords that include a mixture of letters and numbers, to ensure they are not easy to guess or use common combinations. Please do not write down your password or disclose it to anyone else.

(iii) Please do not use your personal devices for work purposes unless this has first been authorised by your Line Manager.

(iv) It is important that you log off your Foundation device or lock the screen when the device is left unattended.

(v) Access to electronic records containing Personal Data must be restricted to Company Personnel for whom access is necessary.

8.4 Security measures for manual records

(i) All manual records containing Sensitive Personal Data must be kept secure in locked cabinets. At the end of the day, please lock these cabinets and keep the key in a secure place.

(ii) Access to manual records containing Personal Data should be restricted to Company Personnel for whom access is necessary.

(iii) When destroying documents in accordance with the Retention Policies or otherwise, please ensure such documents are placed in the shredding bins without delay.

8.5 Working away from the office

(i) If it is necessary for you to work away from the Foundation's premises ("Home Working"), you must only use the Foundation's devices and remote services ("Facilities") when Home Working is related directly to the Foundation and not for personal use. Home Working is only permitted when your Line Manager has given you prior authority to do so and implemented the adequate security measures in respect of the Facilities.

(ii) Please ensure that non-Foundation personnel do not have access to the Facilities or Foundation-related documents or files containing Personal Data ("Company Files").

(iii) Please do not store Company Files on your personal devices unless the IT department has given you authority to do so and implemented adequate security measures, which may include password protection and the installation of up-to-date anti-virus software.

(iv) It is important that you keep Company Files secure when in transit between locations and never leave Company Files unattended. You should keep Company Files separate from personal files and where Company Files are in paper form, these should be kept in a secure place.

8.6 Telephone enquiries

If you deal with telephone enquiries you should be careful about disclosing any Personal Data held by us. In particular you should:

(i) check the caller's identity to make sure that information is only given to a person who is entitled to it;

(ii) suggest that the caller put their request in writing if you are not sure about the caller's identity and where their identity cannot be checked; and

(iii) refer to your head of department and the DPO for assistance.

8.7 Reporting a Personal Data Breach

(i) The GDPR requires Data Controllers to notify certain Personal Data Breaches to the Information Commissioner's Office ("ICO") and, in certain instances, the Data Subject.

(ii) If you know or suspect that a Personal Data Breach has occurred, please do not attempt to investigate the matter yourself, but please contact your head of department and the DPO as soon as possible. Please preserve all evidence relating to the potential Personal Data Breach. It is important that you notify your head of department and the DPO as soon as possible as if we decide the breach needs to be notified to the ICO, this must be done within 72 hours of us/you becoming aware of the breach.

(iii) The DPO shall then take all reasonable steps to mitigate the risk of the Personal Data Breach causing any further damage including but not limited to:

- if relevant, contacting the recipient to request deletion of the relevant document/e-mail and for confirmation of deletion;
- deciding whether the Personal Data Breach needs to be notified to the ICO based on all the circumstances, including whether the breach is likely to present a risk to the Data Subject's rights and freedoms;
- deciding whether the Personal Data Breach needs to be notified to the Data Subject based on all the circumstances, including whether the breach is likely to result in a high risk of adversely affecting the Data Subject's rights and freedoms; and
- investigating the causes of the breach and how the risks of such incidents happening again can be reduced.

It is important that you follow the above procedures to maintain the security of all Personal Data from the point of collection to the point of destruction.

9.0 Transfer limitation

9.1 Before transferring Personal Data to third-party service providers, please consult the DPO. We are only permitted to do so when such third-party service providers agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

We may only share the Personal Data we hold with third parties, such as our service providers if:

(i) they have a need to know the information for the purposes of providing the contracted services;

(ii) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(iii) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place; and

(iv) a fully executed written contract that contains GDPR compliant clauses has been obtained.

9.2 The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not compromised. It is important that you do not transfer Personal Data outside the EEA without first consulting with the DPO.

10.0 Data subjects, rights and requests

10.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to Processing at any time;
- receive certain information about our Processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests;
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the ICO; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a commonly used and machine readable format.

10.2 If a Data Subject contacts you wishing to exercise any of the above rights, please immediately contact your head of department and the DPO.

10.3 If we receive such a request from a Data Subject, the DPO shall follow the below procedure:

(i) upon being notified of the request, take steps to investigate the identity of the individual making the request with the assistance of relevant Company Personnel;

(ii) upon satisfaction that the Personal Data being requested relates to the individual wishing to exercise his or her rights, confirm to the individual that the Foundation is progressing such request;

(iii) liaise with the IT department and other relevant Company Personnel to identify the relevant Personal Data;

(iv) check whether any other individuals' rights and freedoms will be compromised by complying with the request, including whether any Personal Data needs to be redacted; and

(v) consider whether the request must be complied with in the context of the Foundation's other legal obligations and, if so, provide the information to the Data Subject or confirm to the Data Subject the request has been complied with.

We must comply with requests by Data Subjects to exercise the above rights without undue delay and in any event within one month of receiving the request and can only charge a fee in certain circumstances if the request is manifestly unfounded or excessive. In certain situations, we may refuse to comply with a request if it is excessive, but must explain the reason for the refusal to the individual and inform him or her of their right to complain to the ICO and to a judicial remedy.

11.0 Accountability

11.1 Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities.

These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

11.2 Training and audit

We are required to ensure all Foundation Personnel have undergone adequate training to enable them to comply with data privacy laws.

We must also regularly test our systems and processes to assess compliance. Heads of department are responsible for assisting the DPO in ensuring the practices within their department are in accordance with this Policy.

11.3 Privacy By Design and Data Protection Impact Assessments
We are required to implement a concept called "Privacy by Design" when Processing Personal Data. This involves implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with the GDPR.

When implementing such measures, we will take account of the following:

- the cost of implementation;
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

When implementing major new systems within the Foundation, or carrying out the large scale Processing of Sensitive Data, we must carry out a "Data Privacy Impact Assessment". This involves identifying and reducing risks associated with Processing Personal Data.

The DPO and the Club IT department will be responsible for carrying out such Data Privacy Impact Assessments, which must include:

- a description of the Processing, its purposes and our legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

11.4 Direct marketing
We are subject to certain rules and privacy laws when marketing to our customers. For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls).

The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

No Processing that amounts to direct marketing should be carried out without the permission of the Head of Communications and the DPO.

12.0 Implementation

12.1 Information and training

(i) A copy of this Policy is available at the Foundation's SharePoint.

(ii) Guidance on this Policy and data protection generally is available from the DPO. We will periodically train all Company Personnel on data protection matters in line with this Policy and we will ensure that you only Process Personal Data where you have received adequate training to do so. If you require additional training on data protection, please contact the DPO.

(iii) We will ensure that all new Company Personnel are trained on data protection matters in line with this Policy as part of the induction process.

12..2 Monitoring

(i) We are committed to ensuring that this Policy is put into practice and that appropriate working practices are being followed. To this end, the following steps will be taken:

- all Company Personnel who deal with Personal Data will be made aware of data protection issues and encouraged to work towards the continuous improvement of the proper Processing of Personal Data; and

- the DPO shall report to the board of directors on, amongst other things, the level of compliance with or variance from good data protection practices. The board and the DPO will consider what steps, if any, are necessary in order to improve data protection performance.

13.0 Changes to this policy

We reserve the right to change this Policy at any time. Where appropriate, we will notify you of such changes.

Revision	Date	Prepared	Review Date	Further information
1	28.10.2025	MA	28.10.2027	