MFC PRIVACY STANDARD

UPDATED SEPTEMBER 2022

PRIVACY STANDARD – FOR INTERNAL USE ONLY

1. INTRODUCTION

Everyone has rights with regard to the way in which their Personal Data is handled. During the course of our activities we collect, store and process Personal Data about our supporters, customers, suppliers, staff members and other third parties. We recognise that the correct and lawful treatment of this 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. Potential fines of up to approximately **£17.5 million or 4% of total Group worldwide annual turnover** (whichever is higher and depending on the breach) may be incurred for failure to comply with the provisions of the Data Protection Legistaltion.

This Privacy Standard sets out how **MIDDLESBROUGH FOOTBALL & ATHLETIC COMPANY (1986) LIMITED** ("we", "our", "us"), as **Data Controller**, handle all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present Personnel, supporters, customers or supplier contacts, website users or any other Data Subject.

This Privacy Standard applies to all of our Personnel ("you", "your") and sets out what we expect of you. You must read, understand and comply with this Privacy Standard when Processing Personal Data on our behalf. Your compliance with this Privacy Standard is mandatory. Any breach of this Privacy Standard may result in disciplinary action.

This Privacy Standard is an internal document and should not be shared with third parties, or regulators without prior authorisation from the Data Protection Officer ("**DPO**").

2. KEY ELEMENTS

2.1 **Data Protection Legislation** means the **UK GDPR**, **the Data Protection Act 2018**, **the Privacy and Electronic Communications Regulations 2003**, and insofar as it applies the **GDPR**.

2.2 **Data Controller or Data Processor?**

The **Data Controller** is the organisation that **determines the purpose and means** of Processing Personal Data.

A **Data Processor** is responsible for **processing Personal Data on behalf of a Data Controller in the manner and to the extend instructed** by the Data Controller.

We Process Personal Data within MFC for many different purposes. MFC could be Data Controller or Data Processor depending on the circumstances and use of the Personal Data. It is also possible to have joint Data Controllers and numerous Data Processors in any one situation. This must be determined by the DPO and must be documented in our Privacy Notices and contractual agreements.

2.3 **Personal data and Special Category Data**

Personal Data is any information relating to an individual who can be directly or indirectly identified by that data or by associating that data with any other information about them. This includes name, address, date of birth, email address, IP address and cookies. We can only Process Personal Data if a lawful basis for Processing has been identified.

Special Category Data (Sensitive Personal Data) is data consisting of racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; data concerning health; data concerning a natural person's sex life or sexual orientation.

Use of this data requires us to identify additional legal bases for Processing (see below) as the consequences of the Personal Data being lost, stolen, incorrectly or unlawfully used could have a significant adverse impact of the individual.

3. ROLES AND RESPONSIBILITIES

All Heads of Department are responsible for ensuring the Personnel in that Department comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The DPO is responsible for overseeing this Privacy Standard. The DPO is **Iona Sims, Legal Department, 07971050625, data@mfc.co.uk** The DPO should be contacted with any questions about this Privacy Standard or the Data Protection Legislation or if you have any concerns that this Privacy Standard is not being or has not been followed.

You must always contact the DPO in the following circumstances:

(a) if you are **unsure of the lawful basis** which you are relying on to process Personal Data
(b) if you need to **rely on Consent** and/or need to **capture Explicit Consent**
(c) if you need to **draft Privacy Notices**
(d) if you are **unsure about the retention period** for the Personal Data being Processed
(e) if you are **unsure about what security or other measures you need to implement** to protect Personal Data
(f) if there has been a **Personal Data Breach**
(g) if you are **unsure on what basis to transfer Personal Data** outside the UK
(h) if you need any assistance dealing with any **rights invoked by a Data Subject**
(i) whenever you are **engaging in a significant new, or change in, Processing activity** which is likely to require a DPIA or plan to use Personal Data for purposes others than what it was collected for
(j) If you plan to undertake any **activities involving Automated Processing** including profiling or Automated Decision-Making
(k) If you need help complying with applicable law when carrying out **direct marketing activities**
(l) if you need any **contracts in relation to sharing Personal Data** with third parties

4. PERSONAL DATA PROTECTION PRINICPLES

Data Protection Legistaltion require compliance with the following **eight Principles** when Processing Personal Data. We are responsible for and must be able to demonstrate compliance with these Principles.

- **LAWFUL, FAIR & TRANSPARENT** processing;
- **PURPOSE LIMITATION** – Personal Data must be collected only for a specified, explicit and legitimate purpose
- **DATA MINIMISATION** – Personal Data must be adequate, relevant and limited to what is necessary for the purposes for which it is Processed
- **ACCURACY** – Personal Data must be accurate and kept up to date
- **DATA RETENTION** – Personal Data must not kept in a form which permits identification of the Data Subject (individual) for longer than is necessary for the purpose for which the data is Processed
- **SECURITY, INTEGRITY & CONFIDENTIALITY** – Personal Data must be 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
- **TRANSFER LIMITATION** – Personal data must not be transferred to another country without the appropriate safeguards being in place
- **DATA SUBJECTS RIGHTS AND REQUESTS –** we must be transparent in notifying Data Subjects of their rights and have procedures in place to comply with these rights and requests.

4.1 LAWFULNESS & FAIRNESS

Personal Data must be Processed lawfully, fairly and in a transparent manner and for specified purposes. We must only

process Personal Data on the basis of one or more of the lawful bases set out below. **You must identify and document the legal basis being relied on for each Processing activity**. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The specified purposes (lawful bases) are:

4.1.1 **CONSENT - Individual has given his or her consent to Processing – e.g. marketing communications**

Consent requires affirmative action so silence, pre-ticked boxes or inactivity are not sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate.

Individuals must be easily able to withdraw Consent to Processing at any time.

Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the individual first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Category Data, for Automated Decision-Making and for cross border data transfers.

Where Explicit Consent is required, we must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that we can demonstrate compliance with Consent requirements.

4.1.2 **CONTRACT - Processing is necessary for the performance of a contract with the individual to take steps to enter into a contract with them - e.g. ticket, season card holder, product purchases, employment contract.**

4.1.3 **LEGAL OBLIGATION - Processing is necessary to meet our legal compliance obligations .**

4.1.4 **VITAL INTEREST - Processing is necessary to protect the individuals vital interests – health & safety, tax purposes.**

4.1.5 **PUBLIC TASK – processing is necessary to perform a task in the public interest or for our official functions and the take or function has a clear basis in law – e.g NHS test and trace.**

4.1.6 **LEGITIMATE INTEREST - Processing is necessary to pursue our genuine business interests for purposes not overridden by the interests or fundamental rights & freedoms of the individual - e.g fraud prevention, intra-group transfers, IT security, credit checks, certain marketing activities.**

It is important to establish the correct lawful basis for Processing so we can provide people with this information in the Privacy Notice. The lawful basis for Processing can also affect which rights are available to individuals.

	Right to erasure	Right to portability	Right to object
Consent			✖ but right to withdraw consent
Contract			✖
Legal obligation	✖	✖	✖
Vital interests		✖	✖
Public task	✖	✖	
Legitimate interests		✖	

SPECIAL CATEGORY DATA needs more protection because it is sensitive. In addition to establishing a lawful basis, we must identify a separate condition for Processing from the list below:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

TRANSPARENCY (Privacy Notices)

We are required to provide detailed, specific information to Data Subjects whenever we collect Personal Data directly from them. This is done via clear, concise **Privacy Notices** which must be given to the individual when they first provide the data. Our Privacy Notices are available on our website.

Privacy Notices must be regularly reviewed and kept up to date and relevant. All Privacy Notices must be approved by the DPO prior to circulation.

4.2 PURPOSE LIMITATION

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.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

4.3 DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. **Do not collect excessive data.**

You may only Process Personal Data when performing your employment duties requires it. You cannot Process Personal Data for any reason unrelated to your employment duties.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our Data Retention Policy.

4.4 ACCURACY

Personal Data must be accurate and kept up to date. It must be corrected or deleted without delay when inaccurate. You will 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.

4.5 STORAGE LIMITATION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data was originally collected and is Processed.

You must comply with our Data Retention Policy to ensure Personal Data is destroyed or erased after a reasonable time for the purposes for which it was being Processed unless a law requires such data to be kept for a minimum time. This includes requiring third parties to delete such data where applicable. It you are unsure about the data retention period please ask your Manager or the DPO.

4.6 SECURITY, INTEGRITY AND CONFIDENTIALITY

4.6.1 **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. You are responsible for protecting the Personal Data we hold and must exercise particular care in protecting Special Category Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who have a written contract with us, agree to comply with the required policies and procedures and who agree to put adequate measures in place. If you are required to transfer Personal Data **outside the UK** you must consult with the DP to ensure appropriate safeguards are in place prior to the transfer.

You must maintain data security by protecting the:

(a) **Confidentiality**: this means that only people who have a need to know and are authorised to use the Personal Data can access it;

(b) **Integrity**: this means that Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) **Availability**: this means that authorised users are able to access the Personal Data when they need it for authorised purposes

of the Personal Data.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Data Protection Legislation.

4.7 ACCOUNTABILITY – you are required to take responsibility for what you do with Personal Data and how you comply with the principles set out in this Privacy Standard. **Whenever we use a Data Processor or share information with a third party we must have a written contract in place which must include certain provisions set out in the UK GDPR.**

5. REPORTING A PERSONAL DATA BREACH

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately report it to the DPO and the IT Department if is it involves a suspected cybersecurity issue. You should preserve all evidence relating to the potential Personal Data Breach.

MFC is responsible to assess and mitigate the risk of the incident without undue delay. Depending on the circumstances and the risk of harm to the rights and freedoms of the affected individuals, we may be required to notify a Personal Data Breach to the Information Commissioners Office ("**ICO**") within 72 hours of becoming aware of the breach, and, in certain instances, notify the Data Subject. This decision will be made by the DPO after assessment of the incident.

We have in place procedures to deal with any suspected Personal Data Breach set out in the Data Breach Policy.

6. TRANSFER LIMITATION

Data transfers to countries outside the UK are restricted by the Data Protection Legislation. 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.

Individuals' risk losing the protection of the UK data protection laws if their personal data is transferred outside the UK (including to the EU) unless the rights of the individuals are protected in another way or one of the limited exceptions apply.

You may only transfer Personal Data outside the UK if adequate and enforceable safeguards are in place. **Please consult the DPO prior to any proposed or requested transfer of Personal Data outside the UK.**

7. DATA SUBJECT'S RIGHTS AND REQUESTS

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

(a) The right to be **informed** that we Process their data, how and what for, this is provided via our Privacy Notice

(b) The right of **access** to their Personal Data we hold (Subject Access Request)

(c) The right to **rectification** – to correct their Personal Data we hold

(d) The right to **erasure** – if the Personal Data is no longer necessary for the purpose for which it was collected

(e) The right to **restrict processing** or supress their Personal Data

(f) The right to **data portability** to allow individuals to obtain and reuse their Personal Data for their own purposes across different services,

(g) The right to **object** to their Personal Data being used for direct marketing and other certain circumstances

(h) Rights related to **automatic decision making including profiling**

Individuals have a right to withdraw consent and must be allowed to do so easily.

We charge no fee for responses to these requests.

There is no prescribed format for making a request. A person can make a request verbally (to anyone within MFC or in writing). **You must immediately forward any Data Subject request you receive to the DPO and comply with our Data Subject**

response process.

We must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

8. ORGANISATIONAL ACCOUNTIBILITY

We must implement appropriate technical and organisational measures in an effective manner to ensure compliance with the data protection Principles and must demonstrate this via:

8.1 RECORD KEEPING

We are required to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents. This should be recorded on the **Data Processing Record Form** (available from the DPO).

8.2 TRAINING & AUDIT

You must undergo all mandatory data privacy related training and ensure (where applicable) your team undergo similar mandatory training.

You must regularly review all systems and processes under your control to ensure they comply with this Privacy Standard and check adequate controls and resources are in place to ensure proper use and protection of Personal Data.

8.3 PRIVACY BY DESIGN & DATA PRIVACY IMPACT ASSESSMENTS (DPIA)

DPIA are tools and assessments used to identify and reduce risks of a data processing activity.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business changes involving the Processing of Personal Data including:

- use of new technologies or changing technologies (programs, systems or processes);
- Automated Processing including profiling and ADM;
- large scale Processing of Special Category Data;
- high risk Processing; and
- large scale, systematic monitoring of a publicly accessible area.

The DPIA should be conducted in accordance with our DPIA Guidelines (available from the DPO).

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

8.4 CONTRACTS

Whenever a Data Controller uses a Data Processor there must be a written contract containing the data protection clauses compliant with the Data Protection Legislation. Please consult with the DPO.

9. AUTOMATED DECISION MAKING & AUTOMATED PROCESSING

ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Special Category Data are being processed, then grounds (b) or (c) will not be allowed but such Special Category Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

10. 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 (by email, text or post). 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 clearly and separately 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.

11. SHARING PERSONAL DATA

We must not share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

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

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

(b) 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;

(c) the third party is compliant with the required data security standards, policies and procedures and put adequate security measures required under the Data Protection Legislation;

(d) adequate safeguards are in place in respect of any restricted transfers to outside the UK; and

(e) a fully executed written contract that contains data protection clauses approved by the DPO has been put in place.

You must comply with our guidelines on sharing data with third parties.

APPENDIX - DEFINITIONS

Automated Decision-Making (ADM): when a decision is made based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual.

Automated Processing: any form of automated processing where Personal Data is used to analyse or predict aspects concerning an individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements, e.g. profiling.

Consent: agreement - by the Data Subject to the Processing of their Personal Data- which must be freely given, specific, informed and be an unambiguous indication of their wishes, by a statement or by a clear positive action (like an opt in tick box)

Data Controller: the person or organisation that determines when, why and how to process Personal Data.

Data Protection Legislation: Data Protection Legislation means the **UK GDPR, the Data Protection Act 2018** and the Privacy and Electronic Communications Regulations 2003; and insofar as it applies the **GDPR**.

Data Subject: a living, identified or identifiable individual about whom we Process Personal Data.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Personal Data: any information relating to any living individual who can be identified (directly or indirectly) from that data. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Personnel: all employees, volunteers, workers, contractors, agency workers, consultants, directors, members and others.

Privacy Notices: separate notices setting out information that we are required to provide to Data Subjects when we collect information about them.

Processing or Process: any activity that involves the use of Personal Data - obtaining, recording or holding the data, carrying out any operation on the data including organising, amending, manipulating, storing, retrieving, using, disclosing, erasing or destroying it, or transmitting or transferring Personal Data to third parties.

Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers (pseudonyms) so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

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

MFC PRIVACY STANDARD

UPDATED SEPTEMBER 2022

ACKNOWLEDGEMENT OF RECEIPT AND REVIEW

We reserve the right to change this Privacy Standard at any time without notice to you so please check back regularly to obtain the latest copy of this Privacy Standard. We last revised this Privacy Standard on 18 May 2018.

I, [ ], acknowledge that on [ ], I received and read a copy of the Middlesbrough Football & Athletic Company (1986) Limited Privacy Standard and understand that I am responsible for knowing and abiding by its terms. This Privacy Standard does not set terms or conditions of employment or form part of an employment contract.

Signed ……

Name ……

Date ……