Data Protection Policy

Tigers Trust (TT) ("the Company") needs to gather certain information about individuals. These can include customers, suppliers, members, sponsors, corporate business contacts, employees, and other people either Company has a relationship with or may need to contact.

The Data Protection Policy & Procedure seeks to ensure that Tigers Sport and Education Trust:

- Complies with UK data protection legislation and follows best practice
- Protects the rights of staff, customers, and other individuals
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach.

And applies to:

- Permanent, casual staff and volunteers of TT
- All contractors, suppliers and other people working on behalf of TT

It applies to all data that the Company hold relating to identifiable individuals, even if that information technically falls outside of the scope of applicable data protection legislation in the UK (including but not limited to The General Data Protection Regulation and the Data Protection Act 2018) ("DP Legislation").

1. CCTV Policy

Information on the Hull City / SMC Company' use of CCTV, body worn cameras and ANPR technology can be found by requesting a separate CCTV Policy, a copy of which can be accessed on request by email

2. Data Protection Legislation

DP Legislation dictates how organisations including the Company must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or by other methods.

To comply with the law, personal information must be processed in accordance with the principles explained in the following section.

3. Key Terminology used in this policy

3.1. **Processing**, in relation to information or data, means obtaining, recording, or holding the

information or data or carrying out any operation or set of operations on the information or data, including –

- Organisation, adaptation or alteration of the information or data
- Retrieval, consultation or use of the information or data
- Disclosure of the information or data by transmission, dissemination or otherwise making available or
- Alignment, combination, blocking, erasure or destruction of the information or data.

DP Legislation protects the rights of individuals whom the data is about (data subjects), mainly by placing duties on those who decide how and why such data is processed (data controllers).

3.2. **Data Subject** means an individual who is the subject of Personal Data. The Data Subject is the individual whom Personal Data is about.

3.3. **Data Controller** means a person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any Personal Data are, or are to be, processed.

3.4. **Data Processor** in relation to Personal Data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.5. Third Party

A third party in relation to Personal Data, means any person other than –

(a) The data subject

(b) The data controller or

(c) Any data processor or other person authorised to process data for the data controller or processor

In relation to data protection, the main reason for this definition is to ensure that a person such as a data processor, who is effectively acting as the data controller, is not considered a third party.

Although a Data Controller's employee to whom information is disclosed will be a "recipient" they will usually not be a "third party". This is because the employee will usually be acting in their employment capacity, and so will be acting on behalf of the Data Controller.

On a day-to-day basis you may come into contact with or use confidential information about employees, clients, and customers, for example you may deal with personal and/or sensitive data.

3.6. **Personal Data** relates to a living individual who can be identified, this can depend on the data held. Below are examples of Personal Data that you may deal with:

- Names of individuals

- Postal Addresses
- E-mail Addresses
- Telephone Numbers
- Date of Birth
- Recorded opinions about an individual.

It is a requirement of this policy that when processing Personal Data relevant security procedures are in place. For example, if your role involves speaking to supporters over the telephone then identification and verification steps should be made to ensure that you are speaking to the correct person and that information relating to individual is not divulged without completing relevant security checks.
Identification and verification (ID&V) steps should be taken to ensure that security questions are asked when speaking to any data subject that are currently on internal databases. When a data subject needs to be identified the following security questions need to be asked this can be a minimum of 2 questions out of the following criteria:

- Full Name
- First line of address
- Postcode
- Date of Birth
- Contact Telephone Numbers
- E-mail Address
- If a Member, their seat details
- Monthly Payment.

If somebody calls on behalf of another member to purchase tickets, they must be able to supply a customer reference number and pass data protection security. It is best practice to speak to the account holder and get authorisation in all scenarios. For example, if somebody called to move seats, you would need to get authorisation from the payer before completing the move.

3.7. Special Category Data

Special category data relates to Personal Data consisting of information as to:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious or philosophical beliefs

- Whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992):
- Their physical or mental health or condition
- Genetic or biometric data
- Their sexual life and sexual orientation
- The commission or alleged commission by them or any offence; or
- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The processing of special categories of Personal Data is prohibited unless certain conditions are met. In most cases the individual's explicit consent to the processing of such Personal Data will be required. Particular care should be taken when handling special category data.

4. Data Protection Principles:

The main principles of DP Legislation are that Personal Data must be:

- processed fairly and lawfully and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
- accurate and up to date
- kept only for as long as it is needed for the purpose for which it was collected and
- processed in a way that ensures appropriate security of the Personal Data

We are required to demonstrate compliance with the above principles. In addition, Personal Data must be:

- processed in accordance with the rights of the individual to whom the Personal Data relates and
- not transferred outside the European Economic Area unless adequate safeguards have been put in place to allow its export.

All of this means that we and you must take appropriate measures to ensure that Personal Data is kept secure and handled in accordance with the provisions of DP Legislation. You are responsible for ensuring that any Personal Data you provide to us is accurate and up-

to-date and that you inform us of any changes to the Personal Data you have provided.

Please see below for further information about some of the above principles:

4.1. Fair, Lawful and Transparent Processing

The intention of DP Legislation is not to prevent the processing of Personal Data, but to ensure that it is processed fairly and without adversely affecting the rights of the individual to which the Personal Data relates. The individual must be informed about, among other things, the identity of the controller (i.e., HCT or SMC), the purpose for which the Personal Data is to be processed, and the identities of anyone to whom the Personal Data may be disclosed or transferred. Such information must be provided through an appropriate privacy notice or fair processing notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that the individual can understand it.

In order for Personal Data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the individual has consented to the processing, or that the processing is necessary to comply with a legal or contractual obligation, or for the legitimate interest of the controller or the party to whom the Personal Data is disclosed. The processing of special categories of Personal Data (which includes Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data and data concerning health or data concerning an individual's sex life or sexual orientation) is prohibited unless certain conditions are met. In most cases the individual's explicit consent to the processing of such Personal Data will be required.

We will ensure any use of Personal Data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing Personal Data will be aware of the conditions for processing. The conditions for processing relied upon will be available to data subjects in the form of a privacy notice.

4.2. Processing for Limited Purposes

Personal Data may only be processed for the specific purposes notified to the individual when the Personal Data was first collected or for any other purposes specifically permitted by DP Legislation. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the Personal Data is processed, the individual must be informed of the new purpose before any processing occurs.

4.3. Adequate, Relevant and Non-Excessive Processing

Personal Data should only be collected to the extent that it is required for the specific purpose notified to the individual. Any Personal Data which is not necessary for that purpose should not be collected.

4.4. Accurate Data

Personal Data must be accurate and kept up to date. Personal Data which is incorrect, or misleading is not accurate and steps should be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date Personal Data should be destroyed.

4.5. Timely Processing

Personal Data should not be kept longer than is necessary for the purpose it was collected. This means that Personal Data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain Personal Data is likely to be kept before being destroyed or reviewed, please see our separate Data Retention Policy, or contact the Data Compliance Officer.

5. Data Security

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss, destruction, or damage to Personal Data.

DP Legislation requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data may only be transferred to a third-party data processor if the processor agrees to comply with those procedures and policies or puts in place adequate measures itself.

Maintaining information security means guaranteeing the confidentiality, integrity, and availability of Personal Data, as follows:

- "confidentiality" means that only people who are authorised to use the information can access it. Personal Data is always considered confidential
- "integrity" means that Personal Data should be accurate and suitable for the purpose for which it is processed and
- "availability" means that authorised users should only be able to access the information if they need it for authorised purposes.

Common security procedures include (but are not limited to) entry controls, secure lockable desks and cupboards, secure disposal methods, encryption, data minimisation, anonymisation/pseudonymisation and regular IT security checks and backups. Please see below for further details of the data security procedures within the Company. Additional security procedures are also set out in our IT Security Policy.

6. Processing in Line With the Rights of Individuals

Personal Data must be processed in line with individuals' rights. Individuals must be provided with information regarding the processing of their Personal Data and (subject to limited exemptions) have a right to:

- request access to any Personal Data held about them by a data controller (including but not limited to Personal Data held within their personnel file); and
- rectification of inaccurate Personal Data.

In certain circumstances, individuals may also have the right:

- to erasure of Personal Data
- of data portability (i.e., to request the transfer of Personal Data to another party)

- to object to the processing of Personal Data concerning him or her (including to prevent the processing of their Personal Data for direct marketing purposes)
- not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her and
- to restrict the processing of Personal Data (for example to ask to suspend the processing of Personal Data to establish its accuracy or the reasons for processing it)

Any individual wishing to make a request for Personal Data that we hold about them, or any other request of the nature referred to in this section, should be asked to make the request in writing (although in certain circumstances verbal requests may be acceptable). Any member of staff who receives a request (written or otherwise) should forward or refer it to the Data Compliance Officer immediately and not respond directly to the request.

7. Responsibilities

Everyone who works for or with either of the Company has responsibility for ensuring data is collected, stored, and handled appropriately. However, these people have key areas of responsibility:

7.1. **The Company' Data Compliance Officer ("DCO") has overall responsibility for data protection matters within the Company. These responsibilities include**:

- Keeping the board updated about data protection responsibilities, risks, and issues
- Reviewing all data protection procedures and related policies on an annual basis
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with data-related requests from individuals (including requests to see the data either or both of the Company hold about them - also called subject access requests) and
- Checking and approving any contracts or agreements with third parties that may handle Personal Data or any other sensitive data of either of the Company
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure hardware and software is functioning properly
- Evaluating any third-party services the Company consider using to store or process data. For instance, cloud computing services and

- Facilitating impact assessments for any new data, handling processes or data sharing agreements together with the DCO.

7.2. The Marketing Manager is responsible for:

- Approving any data protection statements attached to communications such as e-mails and letters together with the DCO. Addressing any data protection queries from journalists or media outlets like newspapers together with the DCO
- Co-ordinating with the DCO to ensure all marketing initiatives adhere to DP Legislation and the Company' Data Protection Policy and
- Where necessary, working with other staff to ensure marketing initiatives abide by DP Legislation

8. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Compliance Officer.

When data is stored on paper, it should be kept in a secure place so unauthorised people cannot access it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services.
- Servers containing Personal Data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those back-ups should be tested regularly, in line with the Company' standard back-up policy.
- All servers and computers containing data should be protected by approved security software and a firewall.

9. Data Use

Personal Data is of no value to the Company unless the Company can make use of it; however it is when Personal Data is accessed and used that it can be at the greatest risk of loss, corruption and theft:

- The only people able to access data covered by this policy should be those who need it for their work.
- When working with Personal Data, employees should ensure the screen of their computers are always locked when left unattended.
- Personal Data should not be shared informally.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal Data should never be transferred outside of the European Economic Area without authorisation from the DCO.
- Employees should not save copies of Personal Data to their own computers. Always access and update the central copy of data.
- When sending e-mails, all attachments should be password protected and/or encrypted. If personal and/or sensitive information is included in the content of the e-mail this should be in an attachment with above restrictions.

10. Data Accuracy

We will ensure that any Personal Data is accurate, adequate, relevant, and not excessive, given the purpose for which it is obtained. We will not process Personal Data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- The Company will make it easy for data subjects to update information they hold about them. For instance, via the Company' websites.
- Data should be upgraded as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

11. Third Party Requests for Personal Data

Information about our employees, customers, supporters, and other data subjects must not be disclosed to any third party or to the person to whom it relates except in accordance with this policy and our authorised procedures. For example, you must never assume that it is acceptable for a husband to be given Personal Data about his wife; they may be estranged or simply wish to keep their affairs separate. In the event that you receive a request from a third party for disclosure of, or to inspect, Personal Data relating to any individual (including but not limited to employees, customers, or supporters) you should refer the request to the Data Compliance Officer immediately. You should make such a referral in all cases and should not respond to the request regardless of the identity of the requestor (including where the requestor is the police or any other government agency or public authority) as we have a set procedure for responding to such requests that must be followed.

12. Your obligations in relation to personal information

If, as part of your job duties and responsibilities, you collect personal information about employees or other people such as clients or customers, you must comply with this policy. This includes ensuring the information is processed in accordance with DP Legislation, is only processed for the purposes for which it is held, is kept secure and is not kept for longer than necessary. You must also comply with the following guidelines at all times:

- do not disclose confidential personal information to anyone except in accordance with this policy. In particular, it should not be:
    - given to someone from the same family
    - passed to any other unauthorised third party
    - placed on the Company' website
    - posted on the Internet in any form unless the data subject has given their explicit prior written consent to this.
- be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone
- where the Company provide you with code words or passwords to be used before releasing personal information, for example by telephone, you must strictly follow the Company' requirements in this regard
- only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail
- if you receive a request for personal information about any individual, you should forward this to the Data Compliance Officer who is responsible for dealing with such requests

- ensure any Personal Data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons

- do not access another employee's records without authority as this may be gross misconduct and may be a criminal offence

- do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which it would be inappropriate to share with that data subject

- do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by your line manager

- ensure that, when working on personal information as part of your job duties when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and DP Legislation, in particular in matters of data security and

- remember that compliance with DP legislation is everybody's responsibility. If you have any questions or concerns about the interpretation of these rules, please contact the HR Representative immediately.

13. Data protection breaches

It is the responsibility of all employees to report any breaches they become aware of. If you become aware that:

- a device has been lost or stolen, or if you believe that a device may have been accessed by an unauthorised person or otherwise compromised

- there has been unauthorised access to any element of the Company' IT system, premises, or any other location where Personal Data is stored

- any Personal Data has been disclosed or accessed in error

- there is an IT threat (for example, if you have received a phishing email) or

- Personal Data has been compromised in any other way

then in each case you must report the incident to the Data Compliance Officer immediately. In some circumstances we may be required to report the breach to the Information Commissioner's Office and the individual(s) concerned.

14. Queries and Complaints

If you wish to make a complaint that these rules are not being followed in respect of Personal Data either Company holds about you, or have any queries in relation to this policy or how the Company process Personal Data, you should raise the matter with the Data Compliance Officer (who can be contacted by mail, or Data Compliance Officer,

Tigers Trust Arena, West Park, Hull, HU3 6GA).

15. Data Retention

We will only retain Personal Data for as long as we need it for the purpose(s) for which it was collected. Whilst taking in to consideration our legal obligations, we will on an ongoing basis: review the length of time we retain Personal Data; consider the purpose or purposes for which we hold the Personal Data for in deciding whether (and for how long) to retain it; securely delete Personal Data that is no longer needed for such purpose or purposes; and update, archive or securely delete information if it goes out of date. Ensuring Personal Data is disposed of when no longer needed will reduce the risk that will become inaccurate, out of date or irrelevant. Further information and a list of retention periods can be found in the Data Retention Policy (a copy of which can be accessed by email or on the Company' M drive).

16. Additional Information

- This policy does not form part of any employee's contract of employment, and it may be amended by us at any time. Any changes will be notified to you in writing.
- If you are found to be in breach of the terms of this policy you may be subject to disciplinary proceedings which in serious cases, or in cases of repeated breach, may result in dismissal. If you are in any doubt about the terms of this policy or have any questions about data handling, data security, monitoring, or communications, please ask the Data Compliance Officer for further guidance.
- We will continue to review the effectiveness of this Policy to ensure it is achieving its stated objectives.
- The Company will provide training to all employees to help them understand their responsibilities when handling data. Assessments are available for all employees to complete online, which is a mandatory requirement.

Policy Set	CCOP Standard	Policy Name	Approval Date	Review Date
Operations	11. Data Protection	Data Protection Policy	April 2022	3 years By April 2025