DATA PROTECTION POLICY

Our Policies and Procedures are regularly reviewed and updated and have to be approved by the Board of Trustees of the Scunthorpe United CSET and agreed by the Premier League Charitable Fund (PLCF) and the English Football League Trust (EFLT).

1. Overview

1.1 This Data Protection Policy referred to herein as the Trust's 'Privacy Standard' forms part of the Trust's information security framework.

1.2 The Trust recognises and affirms the rights of every individual in respect of their Personal Data. Personal Data. We understand that the correct and lawful treatment of this Personal Data will maintain confidence in the Trust and will support its' successful operation. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that the Trust takes seriously at all times.

1.3 Set out in this Privacy Standard is clear policy, responsibilities and codes of practice which must be complied with when processing Personal Data on the Trust's behalf. Compliance with this Privacy Standard is mandatory and any deliberate or negligent breach of this policy may result in disciplinary action being taken, in accordance with our Disciplinary Policy.

1.4 This Privacy Standard is designed to ensure that the Trust:

a) Protects the rights of all contacts, staff and volunteers;
b) Complies with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security and follows good practice;
c) Is open about what Personal Data it stores and processes and how this is done;
d) Protects itself from the risk of data breach.

2. Why this Privacy Standard exists

This Privacy Standard describes how this Personal Data is to be collected, stored, processed, accessed and disposed of to comply with relevant legislation.

3. Scope

This Privacy Standard:

a) Covers all Person Data held or processed by the Trust, however it is stored, whether in digital media, on paper or any other media;
b) Does not form part of any employee's Contract of Employment and may be amended at any time.

4. Data Protection terms

- **Consent**: Consent is the Data Subject, see below, giving permission for their private data to be processed in a specific way. It means offering individuals real choice and control. Consent requires a positive and clear-cut opt-in - not pre-ticked boxes or any other method of default consent. It should be linked to a clear statement of how the private data will be used (as set out in a Privacy Notice, see below) and how the consent might be withdrawn or altered by the Data Subject at any time.

- **Data**: Information that is stored electronically, on a computer, or in paper-based filing systems.

- **Data Retention Policy**: The Trust's policy which deals with the data, records and documents which the Trust retains and /or disposes of, including electronic documents.

- **Data Subject**: All living identified or identifiable individuals about whom the Trust's holds Personal Data, see below. All Data Subjects have legal rights in relation to their personal information and need not be a UK national or resident.

- **Personal Data**: Data relating to a living individual who can be identified from that data on its own, or when taken together with other information which is likely to come into the Trust's possession. Personal Data can be factual e.g. name or date of birth, or it can be an opinion about that person, their actions and behaviour.

- **Data Controller**: The people who or organisations, such as the Trust, that determine the purposes for which, the manner in which and the reason for which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the GDPR. The Trust is the Data Controller of all Personal Data used in our business for our own charitable purposes.

- **Data Users**: Those of our employees whose work involves processing personal data. Data Users must protect the data they handle in accordance with this Data Protection Policy and any applicable data security procedures at all times.

- **Data Processors**: Any person, organisation or supplier, i.e. third party, that is not a Data User that processes Personal Data on our behalf and on our instructions, e.g. Payroll and Pension administration.

- **Data Protection Manager** (DPM): Person designated by the Trust as responsible for data protection and the implementation of this Data Protection Policy and any applicable data security procedures at all times.

- **General Data Protection Regulation** (GDPR): General Data Protection Regulation (*(EU) 2016/679*) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time. Personal Data is subject to the legal safeguards specified in the GDPR.

- **Privacy Notice**: A separate notice setting out information that may be provided to Data Subjects when the Trust collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals or they may be stand-alone, one-time privacy statements covering processing related to a specific

- **Processing** or **Process**: Any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties, such as information recorded on timesheets for Payroll purposes.

- **Sensitive Personal Data**: Information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, physical or mental health conditions or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings, genetic data and biometric data where processed to uniquely identify a person (e.g. electronic passport photograph). Sensitive Personal Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

5. Data Protection principles

Anyone processing Personal Data must comply with the fair and lawful principles set out in the GDPR. These require that our handling of Personal Data must be:

a) Processed lawfully, fairly and transparently – there must a legal basis for processing Personal Data (which includes obtaining, holding, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it). Processing must be done lawfully, fairly and in a manner open and transparent to the individuals concerned – this includes any transfer of the data to third parties.

b) Collected only for specified, explicit, legitimate and prescribed charitable purposes – these include: project / session monitoring and evaluation, programme course bookings, personnel/employee/volunteer administration, charity and voluntary organisational objectives, public relations, purchase/supplier information, customer/client information and fundraising.

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

d) Accurate and, where necessary, kept up-to-date – every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purpose for which it is Processed, is erased or rectified without delay.

e) Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed; Personal Data may be stored for longer periods insofar as the Personal Data will be Processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

f) Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

g) Protected by design – all procedures and processes need to be designed with data protection in mind. Compliance with legal requirements and good practice needs to be built into the design stage of projects and changes.

6. Legal rights of Data Subjects

GDPR makes clear that the people about whom we hold and Process Personal Data (Data Subjects) have clear legal rights as set out in the next section. As well as complying with the requirements for security and transparency, the Trust has to have a legal basis for processing Personal Data, as set out below:

a) The Data Subject has given their consent;

b) Processing is necessary for the performance of a contract with the Data Subject;

c) For compliance with a legal obligation to which the Trust is subject;

d) To protect the vital interests of the Data Subject;

e) Processing is necessary for a task carried out in the public interest or in the exercise of official authority;

f) For the legitimate interests pursued by the Trust or a third party (except where these interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

A Data Subject consents to the 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 insufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. 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 Data Subject first consented.

Unless we can rely on another legal basis of processing, explicit consent is usually required for processing Sensitive Personal Data. Where Explicit Consent is required, you must issue to the Data Subject a separate Privacy Notice to capture explicit consent.

When Sensitive Personal Data is being processed, additional conditions must be met. Clear legal grounds are required to Process Sensitive Personal Data and any consent must explicitly cover the sensitive data being processed.

7. Notifying Data Subjects

If we collect Personal Data directly from Data Subjects, we will inform them about the purpose or purposes for which we intend to process their Personal Data and the legal basis for processing, provided through appropriate Privacy Notices.

We will also explain their rights, including:

a) The right to be informed;
b) The right of access;
c) The right to rectification;
d) The right to erasure;
e) The right to restrict processing;
f) The right to data portability;
g) The right to object;
h) The right not to be subject to automated decision-making

The Trust will only collect Personal Data to the extent that it is required for specified, explicit and legitimate 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.

The Trust will ensure that Personal Data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

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

We will only Process in line with the Data Subjects' rights and in particular their rights to:

a) Withdraw consent to processing at any time;
b) Request access to their Personal Data held about them;
c) Prevent our use of their Personal Data for direct-marketing purposes;
d) Ask to have inaccurate Personal Data amended;
e) Request the deletion or removal of Personal Data where there is no compelling reason for its continued processing;
f) Prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
g) Obtain and reuse their Personal Data for other purposes.

9. Data security

The Trust will ensure that Personal Data is processed securely and in line with its' Information Security Policy.

10. Data accuracy

Every effort will be made to ensure Personal Data is accurate and, where necessary, kept up-to- date. It must be corrected or deleted without delay when inaccurate. It must be relevant to the purpose for which it was collected. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

11. Data retention and storage

Personal Data will only be stored and held in line with the Trust's Data Retention Policy.

12. Disclosure and sharing of Personal Data

The Trust will not share Personal Data with our third party service providers except to carry out our obligations under any contract, such as Payroll purposes, or for our legitimate interests. Apart from these service providers the Trust will not share or exchange the Personal Data it holds with other organisations.

We will share Personal Data if we are under a duty to disclose or share a Data Subject's Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

13. Subject Access Requests (SAR)

Data Subjects have a right to have a copy of all of their Personal Data we are holding. They need to make a formal request in writing. The Trust will meet the request in full within one calendar month uncles the request is complex or numerous in which case the period in which we must respond can be extended by a further two months and no charge will be levied on anyone requesting their Personal Data. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

14. Transferring Personal Data to a country outside the United Kingdom (UK)

The Trust will not transfer any Personal Data to a country outside the UK without your express consent.

15. Data security breaches

The Trust will notify to the applicable regulator, the Information Commissioner's Office (IOC) within 72 hours of becoming aware of any breach, including full and accurate details of the incident, including what class of data is involved an, in certain circumstances, to the Data Subject, any breach that may compromise the security, confidentiality or integrity of Personal Data.

16. Children and young people's data

The GDPR required that permission from a parent/legal guardian is required before a child / young person's Personal Data can be processed. Parent consent is required for children below the age of 13 years old.

The Trust will ensure that parent permission will always be sought before Personal Data is collected and processed. Further information is available in the Trust's Website Privacy Notice, a copy of which can be obtained from the Data Protection Manager.

17. Privacy by design and Data Protection Impact Assessments (DPIA)

The Trust is required to implement privacy by design measures when processing Personal Data by implementing appropriate technical and organisational measures in an effective manner.

Data Controllers must also conduct DPIAs in respect of processing likely to result in high risk to a Data Subject, e.g.:

a) Where a new technology is being deployed;
b) Where a profiling operation is likely to significantly affect Data Subjects; and
c) Where there is processing on a large scale of Sensitive Personal Data.
d)

If a DPIA indicates that the processing is high risk, then the situation will need to be referred to the Data Protection Manager who will consult the ICO to seek its opinion as to whether the processing operation complies with GDPR.

18. Staff and volunteer training

All Trust staff and any volunteers (including those on Work Experience) required to access or handle Personal Data will be trained every six months in data protection good practice and will be required to read this Privacy Standard as part of their Induction. Staff will sign to say they have understood the Privacy Standard/training and a copy will be kept in their HR file.

19. Privacy Notices

The Trust is to provide detailed, specific information to Data Subjects through relevant Privacy Notices setting out what Personal Data is held and processed, the reasons for this and the legal basis together with how their rights in law are being upheld by the Trust.

20. Control and review

The Trust's Data Protection Manager should undertake data protection compliance checks, at least annually and, if and when, as requested by the Board of Trustees.

Similarly, the Data Protection Manager should undertake appropriate compliance checks with staff and volunteers. The frequency of such checks will be decided by the Board of Trustees.

Any data protection issues requiring a decision will be recorded by the Data Protection Manager on a Log and stored securely.

21. Fundraising policy and practice

The Trust's approach is to be legal, open, honest and respectful in all our fundraising activities. We do not engage in fundraising that might involve unreasonable intrusion on a person's privacy or is unreasonably persistent. Funds raised for a particular activity are used for that activity and our accounting system is designed to provide for this through a system of accounts for restricted funds. All our fundraising practices comply with the Code of Fundraising Practice issued by the Fundraising Regulator.

22. Responsibilities

The Trust is responsible for and able to demonstrate compliance with the legal requirements and the principles set out above, with the Board of Trustees responsible for ensuring that this core Privacy Standard is implemented in the Trust's work.

The Data Protection Manager is responsible for and able to demonstrate compliance with the principles and policies set out in this core Privacy Standard.

Staff and volunteers are responsible for understanding and following the principles, practices and procedures set out for them by their Data Protection Manager through appropriate training.

23. Changes to this Privacy Standard

The Trust reserves the right to change this Privacy Standard at any time. Where appropriate, we will notify Data Subjects any relevant changes affecting them.