DATA PROTECTION POLICY

Littlewood Group complies with all applicable laws in connection with processing data, including the General Data Protection Regulation (GDPR) and Data Protection Act 2018. Our data protection standards are underpinned by this policy as well as our Code of Conduct. Data users are obliged to comply with this policy when processing personal data.

Data Protection Definitions

- Data is information which is held electronically, or in paper-based filing systems.
- Data Subjects for the purpose of this policy include all living individuals about whom we hold personal data.
- Personal Data means data relating to a living individual who can be identified from that data (or in combination with other information in our possession). Personal data can be factual (such as a name, employee number or date of birth) or it can be an opinion about that person, their actions and behaviour.
- Data Controllers are the decision makers over the processing of personal data. They exercise control over the purposes and means of any processing.
- Data Processors processes personal data on the instruction of a data controller.
- Data Users are those employees (hereafter referred to as those people employed by Littlewood Group and those working on Littlewood Group premises / infrastructure and where Littlewood Group policies are applicable) whose work involves processing personal data.
- Processing is any activity that involves use of data. It includes collecting, recording, or holding the data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring personal data to other parties.
- Special Category Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, genetic data, or biometric data, physical or mental health or condition or sexual life or sexual orientation (and such other categories as may be added from time to time). Special category personal data can only be processed under certain conditions.
- DP Legislation refers to any current or future laws or directives that are or will be applicable in the UK with respect to data processing. This includes the Data Protection Act 2018 and the General Data Protection Regulation.

Data Protection Principles

Anyone processing Personal Data must comply with the six principles for processing Personal Data as contained within DP Legislation. These provide that Personal Data must be:

Processed fairly, lawfully, and transparently.

Personal Data must be processed in a way that is not unduly detrimental, unexpected, or misleading. Personal Data may only be processed if there is legal ground for that processing. One of the following conditions must be met:

I. Performance of a contract (for example, an employment contract in respect of Littlewood Group employees or a service contract in the case of services to clients).

II. Legal obligation (where Processing is required to comply with a common law or statutory obligation)
III. Legitimate interest (applicable where Littlewood Group or the wider society has a benefit in processing Personal Data and where such processing is balanced against the rights and freedoms of individuals)
IV. Consent (where the Data Subjects have given their permission to process their Personal Data)

If the processing you are considering does not fall under one of the conditions above, then contact the HR Department for further guidance.

Personal Data must be processed in an open and honest manner. Individuals must be informed as to how their data is processed.

When Special Category Personal Data is required to be processed, additional conditions to those set out above must also be met. If you are intending to process Special Category Personal Data, please contact the HR Department.

Processed for a specified purpose

The purpose(s) of the Processing must be clear from the start and must be recorded.

Minimised

The data collected must be adequate, relevant, and limited to what is necessary to fulfil the stated purpose(s) of the Processing.

Accurate

Steps must be taken to maintain the accuracy of data, including correcting information that is incorrect or misleading. Littlewood Group employees are responsible for notifying the HR Department immediately of any changes to their personal circumstances.

Not kept for longer than necessary for the purpose and processed securely

All Personal Data is classified as ‘Confidential’ (information that must not be disclosed unless appropriate). This principle means that Personal Data must be kept secure by maintaining the confidentiality, integrity and access to the data. Data Users must employ reasonable security measures including, where appropriate and/or relevant:

- Access control (into a building/premises)
- Physical storage locking controls
- Electronic folder restrictions
- Encryption
- Littlewood Group-approved file transfer methods
- Secure Personal Data destruction

In complying with this principle Data users are required to adhere to the Littlewood Group Information Security Policy.

Personal data must be processed in a manner that will enable Littlewood Group to demonstrate accountability in meeting each of the six principles outlined above.

Transferring Personal Data outside the UK

The Managing Director must approve in writing where a transfer of Personal Data outside the UK is being proposed. Personal Data may only be transferred under certain conditions, including ensuring that Data Subject Rights are maintained.

Data Sharing

Personal data may be shared within Littlewood Group, or externally, only on a need-to-know basis and so long as the Data Subject is informed.

Data Subjects whose data is shared may only have that data shared if it is in accordance with the Data Subject Consent Form and they have signed the Data Subject Consent Form.

In addition, Personal Data may only be disclosed externally if there is a legal basis (e.g. a legitimate interest, legal obligation or to comply with a contract).

Before sharing Personal data there are a number of factors that the Data User must consider:

I. The objective – this will help to provide clarity on what data needs to be shared, if any, and to whom.
II. Data required – the data that is shared must be minimised to the data that is required
III. Recipients of data – data should only be shared on a 'need to know' basis
IV. Frequency of data sharing – Personal Data should not be shared more frequently than necessary. Data users must consider whether it is appropriate to share data on an exceptional basis, on-going or routinely.
V. Mode of sharing – data must be shared in a secure manner.
VI. Risk of sharing Personal Data – data users should consider risks to the Data Subjects
VII. Anonymising data – data users should consider if the objective can still be achieved by anonymising data.
VIII. Transfer of data outside the UK – Personal Data must not be transferred outside the UK without authorisation from the Managing Director.

Data Transmission

Data transmission is the transfer of data from one location to another. It comprises the transmission of physical data and electronic data.

Physical transfer of data carries with it greater Personal Data risk due to the inherent lack control in the event of a potential data breach. Physical data transfers should only be carried out where there is no electronic alternative available or if it would not be practical to transfer the data in another manner.

The duration of the transit period, when transferring from one Littlewood Group location to another, should be kept to a minimum to lower the risk of a potential data breach.

Physical data that is required to be posted must be sent in a secure manner. This will typically be via point-to-point Courier.

Where electronic transfer is appropriate, it is required to be transferred securely and through a Littlewood Group approved means of transfer such as OneDrive (or, in some cases, by use of an FTP server such as WeTransfer).

Data Retention

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. Reference should be made to the Littlewood Group Personal Data Consent Form for details of retention periods. We will take all reasonable steps to destroy or erase from our systems all data which is no longer required.

Video images – CCTV

CCTV is generally regarded as a privacy intrusive method of monitoring and should therefore only be considered for use once other alternative options (that may be less intrusive) have been considered and are deemed unsuitable. The appropriateness of any CCTV systems that are already in operation, should be reviewed periodically to check that its use remains appropriate and that it meets the purpose for which it was installed.

The system must be operated in a way that is consistent with the rights and freedoms of individuals (i.e. does not cause harm to individuals).

CCTV must be located at strategic points and must be focused / positioned to capture images of interest.

In the case of static CCTV, these should be pointed towards or in the immediate vicinity of Littlewood Group property (or the property of the client where we are working) or, where operated on vehicles, specifically towards the area that is the focus of the monitoring.

Appropriate legible signs must be placed in prominent locations to inform those whose images may be captured that CCTV is in operation.

Designated owners (or a delegate) of the CCTV system must complete the checklist for installation and maintenance of CCTV systems.

Access to CCTV footage must be restricted to persons with a legitimate requirement to view it. It should not be placed on public display. CCTV footage must be deleted when its' purpose is obsolete. 14 days is an acceptable time limit for most footage, however, footage capturing scenes of interest (e.g. theft, employee misconduct or HSE incident) may kept until its' purpose is served.

Drones

Drones may be operated in limited circumstances and in certain locations. The primary purpose of operating drones must be in connection with enhancing commercial operations rather than a collection of Personal Data.

Users are required to comply with all applicable laws (including those from the Civil Aviation Authority) relating to the use of unmanned aircraft and any licencing requirements. Where specific permissions are required, users are required to obtain and comply with those permissions.

Before considering use of drones Data privacy risks must be assessed.

Data Subject's rights under Data Protection Legislation

Littlewood Group will process all Personal Data in accordance with Data Subjects' rights where it is applicable, and in particular their right to:

A request to have inaccurate data amended
B request access to any data held about them by a data controller
C be informed about how their Personal Data is processed
D prevent the processing of their data for direct-marketing purposes
E object to the processing of their Personal Data in certain instances
F restrict the processing of their Personal Data in certain instances
G withdraw their consent in the case where consent had previously been granted
H request erasure in certain instances

All Data Subject Requests will be submitted using form LWPT20D Personal Data Subject Access Request. In most cases, we are required to comply with any Data Subject request within 1 month of the request being submitted. In the case of requests to have inaccurate data amended form LWPT20D does not need completing.

Data breaches and complaints

A potential data breach is an incident in which sensitive, confidential or otherwise Personal Data has been accessed, disclosed or handled in a manner inconsistent with the intended treatment of that information.

A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. This includes breaches that are the result of both accidental and deliberate causes.

A non-comprehensive list of potential data breach examples includes:

- Unauthorised deletion of data
- Sending data to an unintended recipient
- Access to data by an unauthorised individual
- Sending Littlewood Group confidential data to a personal email address for non-business use
- Loss or theft of a laptop
- Alteration of data without permission
- Misplacing data
- Cyber attack

Data breaches may also include cases where Data Subjects' rights are not managed appropriately.

It is important that we are able to deal with any data incident as soon as possible to effectively manage the incident. As such, all Littlewood Group employees must notify the HR Business Partner immediately after becoming aware of any data incident. In no circumstances should you communicate details of the incident outside of those managing the data security incident without first contacting the HR Business Partner.

The HR Business Partner, Compliance Manager and nominated Director will consider the potential data breach facts as presented. They will determine the course of action to take according to the findings.

Consequences of breaching this policy

Non-compliance with this policy by employees may result in disciplinary action up to and including summary dismissal, and by contractors or agents to termination of contract.

Speaking up

If you have a concern or suspect a violation of this policy, we want you to speak up immediately. Speaking up can be a difficult thing to do, so be reassured that all information received will be treated seriously and investigated appropriately. If you act in good faith, believing your information is accurate, we will protect you even if you are wrong. Some concerns can be addressed by speaking to the person whose conduct is the cause for concern. We understand that this is not always possible, so we suggest that you speak to your Departmental Director. If, for whatever reason, you do not feel comfortable doing this, you can contact any member of the HSEQ or HR Department.

Signed on behalf of the Board of Directors,

Jon Hobden
Managing Director
Date of Review: 10th October 2025 **Next Review: 10th October 2026**