**1.6 GDPR & Data Protection**

## REGULATIONS AND STANDARDS

**SCOPE OF THIS CHAPTER**

Leyton Green is committed to being transparent about how it collects and uses the personal data of its employees and contracted individuals as well as its clients, and to meeting its data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal and professional data of clients, employees, contractors, volunteers’ former employees.

This policy also has relevance in principle to the personal data of clients and other personal data processed for business purposes.

## Contents

**1. Definitions**

**2. Data Protection Principles & Training**

**3. Individual Rights**

**4. Other Rights**

**5. Data Security**

**6. Record Keeping**

**7. Data Breaches**

**8. International Data Transfers**

**9. Individual Responsibilities**

**10. Data Retention and Disposal**

**11. Email Policy - Email Acceptable Usage**

**12. Disclosure of Information**

## 1. Definitions

***"Personal data"*** is any information that relates to a living individual who can be identified from that information.

***“Processing”*** is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.

***"Special categories of personal data"*** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

***"Criminal records data"*** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

# 2. Data Protection Principles & Training

Leyton Green processes HR-related personal data and personal data in accordance with the following data protection principles:

* Leyton Green processes personal data lawfully, fairly and in a transparent manner.
* Leyton Green collects HR-related personal data and personal data only for specified, explicit and legitimate purposes.
* Leyton Green processes HR-related personal data and personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.
* Leyton Green keeps accurate HR-related personal data and personal data and takes all reasonable steps to ensure that inaccurate HR-related personal data and personal data is rectified or deleted without delay.
* Leyton Green personal data and personal data only for the period necessary for processing.
* Leyton Green adopts appropriate measures to make sure that HR-related personal data and personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

Leyton Green tells individuals the reasons for processing their HR-related personal data and personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

HR-related personal data and personal data may be processed only if the data subject has given his or her consent or where Leyton Green processes special categories of HR-related personal data and personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

Leyton Green will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment relationship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the Leyton Green holds HR-related personal data are contained in its privacy notices to individuals and related policy.

Leyton Green keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

**Training**

Leyton Green will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

# 3. Individual Rights

As a data subject, individuals have a number of rights in relation to their personal data**.**

**Subject Access / Omission Requests**

Individuals have the right to make a subject access / omission request. If an individual makes a subject access / omission request, Leyton Green will tell him/her:

* Whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual.
* To whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers.
* For how long his/her personal data is stored (or how that period is decided).

Under the regulations of the General Data Protection Regulations 2018, employees may request to view information held on their personnel files, including references from previous employers. These may be disclosed where Leyton Green considers it reasonable to do so. However, where it is not felt appropriate to do so, for example where there would be a risk of violence to the referee, Leyton Green reserves the right to seek the referee’s consent to disclose the reference. In such cases, if the referee refuses consent, Leyton Green will exercise its right to withhold the information. However, in keeping with best practice, even where the referee has refused consent, Leyton Green may disclose factual elements of the reference such as dates of employment etc.

An employee’s or any contracted individual undertaking works for Leyton Green, personal data will not be made available to other parties, other than to provide e.g. Managers / Administrators with information reasonably required in their role.

# 4. Other Rights

Individuals have several other rights in relation to their personal data. They can Leyton Green to:

* Rectify inaccurate data.
* Stop processing or erase data that is no longer necessary for the purposes of processing
* Stop processing or erase data if the individual's interests override Leyton Green legitimate grounds for processing data (where Leyton Green relies on its legitimate interests as a reason for processing data)
* Stop processing or erase data if processing is unlawful; and
* Stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override Leyton Green legitimate grounds for processing data.

To ask Leyton Green Ltd to take any of these steps, the individual should make a request

# 5. Data Security

The organisation takes the security of HR-related personal data and personal data seriously. The organisation has internal policies and controls in place to protect HR-related personal data and personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

**Data Storage**

All data, other than Public data, must be stored securely.

Leyton Green can keep copies of HR-related personal data and personal data both in hard copies and electronic copies. In both cases, Leyton Green is committed to the safe and secure storage of information.

Manual records such as client files, which would include matters such as signed service agreements, are be kept in locked facilities. must be taken when working on confidential sensitive client or personnel files.

Where data is stored electronically on a computer the following steps should be considered:

* Check periodically on the accuracy of data being entered.
* Ensure that the computer system is secure by checking that it has a backup system, that lost data can be recovered and that backups are stored in a safe and secure place.
* Ensure that all employees who need to use the computer system are thoroughly trained in its use.
* Ensure that passwords are being used for access to different parts of the system, that these are regularly changed and not abused by being passed onto people who should not have them.

# 6. Record Keeping

Leyton Green and its employees and contracted individuals keep records to fulfil their statutory and contractual obligations. This will include, for example, areas such as: Health and Safety; employment law; legal protection; finance; fundraising; social services and all types of support related records. Leyton Green to preserving the right to confidentiality of all individuals or groups. However, Leyton Green does reserve the right to share information without prior consent where there is a real and identifiable concern for an individual’s or group’s safety and wellbeing.

# 7. Data Breaches

If Leyton Green discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Leyton Green will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

# 8. International Data Transfer

The organisation does not currently transfer HR-related personal data to countries outside the EEA. If it were to (e.g., in relation to cloud based HR systems) transferred outside the EEA in the future it would be on the basis of prior implementation all relevant safeguards e.g. declaration of adequacy and binding corporate rules.

## 9. Individual Responsibilities

Individuals are responsible for helping Leyton Green keep their personal data up to date. Individuals should let Leyton Green know if data they have provided changes, for example if an individual moves to a new house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our customers, clients, and service users in the course of their employment, contract, volunteer period, or apprenticeship. Where this is the case, Leyton Green relies on individuals to help meet its data protection obligations to staff, customers, clients and service users.

**Individuals who have access to personal data are required:**

* To access only data that they have authority to access and only for authorised purposes.
* Not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation.
* To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction).
* Not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
* Not to store personal data on local drives or on personal devices that are used for work purposes; and
* To report data breaches of which they become aware to Raul Jaque or in his absence Abigail Adieze immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under Leyton Green disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to summary dismissal without notice.

## 10. Data Retention and Disposal

**Introduction**

Leyton Green approach is to take any statutory minimum retention period as the default retention period and then determine if there are any justifiable reasons for longer retention periods to be used.

***Recruitment Records***

The vacancy filler recruitment site is set to automatically purge candidate data after 1 year.

The HR team delete / destroy all data relating to unsuccessful candidates 6 months after the completion of the recruitment process – this allows for any queries or complaints to be investigated and resolved.

***HR – Employment Records***

Employment records for all staff are retained for 10 years after the end of the financial year in which their employment concluded– this period enables accurate referencing to be provided for a significant period post- employment which we consider to be important considering our role as a significant employer in the sector.

Archiving will be organised to enable “ staff” records to be retained for 10 years but Retail and Support staff records to be disposed of 7 years after the end of the financial year in which their employment concluded.

***National Minimum Wage and General Payroll Records***

The minimum period of retention for this category of record is generally three years from the day of the pay reference period immediately following that to which the records relate. Leyton Green policy is to keep these records for 6 years following the end of the financial year to which the record relates – this enables any potential query or civil claim arising from e.g. NMW to be properly investigated.

***Financial Records***

Leyton Green policy is to retain all relevant finance related records for a period of 6 years after the end of the relevant financial year end – this position meets or exceeds the minimum retention period for all categories of financial data and simplifies the archiving and subsequent disposal of records.

***Health and Safety Records***

These records are archived for disposal 15 years after the end of the financial year to which they relate. Should there be any records relating to e.g., exposure to Asbestos or specified hazardous substances these would be retained for a period of 40 years.

**Children and Young People’s Support Records**

|  |  |  |  |
| --- | --- | --- | --- |
| **Subject** | **Record** | **Reference** | **Retention Period** |
| **Looked After Children** | Case records for looked after children. | Planning, Placement and Case Review (England) Regulations 2010, s. 50. | Either:  until the **75th anniversary** of the child’s birth, or  if the child dies before age 18, for **15 years** from the date of death. |
| **Children’s Homes** | Children’s case records for children accommodated in children’s homes. | Children’s Homes (England) Regulations 2015, Regulation 36. | Either:  until the **75th anniversary** of the child’s birth, or  if the child dies before age 18, for **15 years** from the date of death. |
| **Child Protection/ Assessments/ Referrals/ Children in Need/Serious Case Reviews** |  | No specific legislative retention period.  Under the Limitation Act 1980, there is generally a statutory limitation period of 6 years in which civil claims may be instituted.  In the case of children, this time does not start to run until age 18. The suggested retention periods are in accordance with this limitation period. | Either:  until the **25th anniversary** of the child’s birth, or if the child dies before age 18, for **6 years** from the date of death. |

***Data Disposal***

***Hard Copy***

Personal data, Sensitive Personal data and organisation specific data must all be disposed of via secure shredding services – if in doubt shred.

***Electronic Data***

***Individuals***

Individual users are responsible for routinely disposing of data they hold in their Leyton Green email account through deleting unneeded emails and then completing the deletion process by also deleting the email from the deleted items folder.

Each user is responsible for deleting unwanted items from their “desktops” and then completing the double deletion process by also deleting the item from the desktop “trash can”

If any data stored in Leyton Green “Cloud Backup” is no longer required, this should also be deleted. Leyton Green review the information stored within the Leyton Green “Cloud Backup” method on an annual basis. Any data no longer required is deleted unless in disagreement with statements within the Leyton Green GDPR Policy as stated above or the remainder of this Policy.

## 11. Email Policy & Email acceptable Usage

***Scope of E-mail Policy and Objectives***

The purpose of this policy is to provide information about Leyton Green email services and to provide guidelines for users on the secure, effective, and acceptable use of email. This policy also describes the standards to be complied with when using these facilities for email, and to ensure that users are aware of the legal consequences attached to the inappropriate use of the facilities.

Email is a communication tool, and all users must use email in a responsible, effective, and lawful manner.

Email is provided as part of Leyton Green overall provision of IT facilities; Email is subject to relevant legislation.

This policy applies to the use of email for the purpose of sending or receiving email messages and attachments.

This policy is in place to prevent abuse of Leyton Green email system and to Leyton Green from any compromise of confidential information or potential legal liability. It is the responsibility of all staff, volunteers and individuals undertaking works for Leyton Green to comply with this Policy. Leyton Green has the right to intercept access or review the contents of any email; electronic communication or files created and monitor usage on a random basis. This will be for the purposes of preventing, detecting, or investigating crime or misuse, ascertaining compliance with regulatory standards and Leyton Green policies, or to secure effective system operation.

Leyton Green has the legal right to monitor usage of the e-mail system, using the least intrusive method available, and reserves the right to disclose the contents of any email or other electronic communications to comply with or assist law enforcement officials or legal authorities.

**Access**

Authorised users are issued with an email account by Leyton Green. This account should be secured by the user with a personal password. An email account may only be used by the person to whom it is assigned and is not to be shared with anyone for any reason. Your account and password should be protected accordingly to prevent abuse. You will be held responsible for any illegal activity that occurs from the use of your account.

In some circumstances legitimate access may be allowed to another person’s email accounts by e.g., Leyton Green Senior Management in the event of long-term absence due to serious illness. Such access to a user’s account in these instances must be approved by the Directors of Leyton Green Access must not normally be granted in the case of short-term absence. Every user is responsible for ensuring that appropriate arrangements are made to cover periods of absence.

***Email Account Closure***

When a member of staff leaves the employment of Leyton Green their email account is cancelled as part of the termination process.

User Accounts to be closed are subject to the following conditions:

* Staff should ensure that they unsubscribe from any email lists that they have subscribed to. If there are any work-related emails that need transferring to another user, then these emails should be forwarded as appropriate.
* If a member of staff is dismissed from employment due to misconduct - the account is immediately closed. Any data stored under their account can be released upon appropriate authorisation.
* Leyton Green reserves the right to redirect/allow access to the email accounts for legitimate purposes of those staff that have left.

***Acceptable Use***

Email should be as carefully constructed as per other types of correspondence.

The users of the email system are responsible for ensuring that they are acting in compliance with legal and acceptable use conditions. It should be noted that email messages (deleted or otherwise) may be treated as written evidence in law.

Users should ensure that email messages:

Are courteous and polite.

Protect others’ right to privacy and confidentiality.

Leyton Green Management under the white cottage Children’s Home, will exercise its discretion in judging reasonable bounds within the above standards for acceptability of material transmitted by email.

Leyton Green regards the declaration of standards, as described above, to be particularly important. They reflect the values of the company.

***Preventing the Spread of Malicious Software (Viruses)***

Users of Leyton Green systems must take all reasonable steps to prevent the receipt and transmission by email of malicious software e.g., computer viruses.

Users

* Must not transmit by email any file attachment which they know to be infected with a virus
* Must ensure that an effective anti-virus system is operating on any computer which they use to access Leyton Green IT facilities
* Must not open email file attachments they have received from unknown, unsolicited, or un-trusted sources.
* Must use encryption software where feasible and always for Confidential sensitive and Commercially secret Data.

***Personal Use***

Leyton Green anticipates that many users have IT access outside of work and that in this case there would be little need to use Leyton Green email for personal messages. Leyton Green does not permit the use of Leyton Green email system for personal messages.

***Unacceptable Use***

The main purpose for the provision by Leyton Green of IT facilities for email is for the use in connection with the work of Leyton Green

IT facilities provided by Leyton Green for email should not be used:

* For the creation or transmission (other than for properly supervised and lawful information research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
* For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience, or needless anxiety.
* For the creation or transmission of material that is abusive or threatening to others or serves to harass or bully others
* For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs. Leyton Green is committed to fostering a working environment free of discriminations where everyone is treated with dignity and respect.
* For the creation or transmission of defamatory material

***Implementation***

* Leyton Green will do its best to ensure that employees of individuals undertaking works for Leyton Green access and use email in accordance with this policy.
* Users who fail to follow this policy risk disciplinary action and possible termination of employment.
* Leyton Green acknowledges its obligation to report any illegal activities to the appropriate authorities.
* Unless informed otherwise, Leyton Green assumes that all users understand this policy and accept personal responsibility for adhering to its requirements.

***Legislation***

The following are some of the areas of law which apply to the use of email, and which could involve liability of users or Leyton Green

* ***Intellectual Property***

Anyone who uses email to send or retrieve any materials that infringe the intellectual property rights of a third party may be liable to that third party if such use is not authorised by them.

***Obscenity***

A criminal offence is committed if a person publishes any material which is pornographic excessively violent or which comes under the provisions of the Obscene Publications Act 1959, and the Protection of Children Act 1978. The Protection of Children Act 1999 makes it an offence to publish or distribute obscene material of a child.

* ***Defamation***

As a form of publication, the Internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation.

* ***Data Protection***

Processing information including photographs which contains personal data about individuals requires the express written consent of those individuals. Any personal data beyond that registered with the Information Commissioner will be considered illegal.

* ***Copyright***

The Copyright, Design and Patents Act 1988 are applicable to all types of creations, including text, graphics and sounds by an author or an artist. This will include any which are accessible through Leyton Green IT facilities.

* ***Discrimination***

Any material disseminated which is discriminatory or encourages discrimination may be unlawful under the Sex Discrimination Act 1975, the Race Relations Act 1976, the Disability Discrimination Act 1995, the Human Rights Act 1998 or Employment Equality (Religion or Belief/Sexual Orientation) Regulations (2003) where it involves discrimination on the grounds of sex, sexual orientation, religion, race or disability.

## *12. Disclosure of Information*

***Introduction***

Leyton Green works with vulnerable members of society and as such employees or individuals conducting work on behalf of Leyton Green often have access to sensitive personal information relating to service-users and their families. Additionally, as with any service-provider elements of our records are commercially sensitive. Leyton Green is committed to maintaining the highest standards of integrity where disclosure of information is concerned.

* No employee shall directly or indirectly disclose to any unauthorised person any knowledge or information relating to Leyton Green activities, or the details about any Leyton Green clients, residents, guests, volunteers, or supporters without first obtaining permission in writing from the relevant Leyton Green Manager.
* No employee will use, for their own purposes, or profit or for any purposes other than those of Leyton Green, any information, which may be acquired in relation to Leyton Green and/or its clients, residents, guests, volunteers, or supporters.
* The rules concerning disclosure of information apply both during and after an employee’s employment with Leyton Green
* Unauthorised access to Leyton Green information, whether computerised or manual, may lead to disciplinary action. In the case of computerised information "hacking" may be considered a dismissible offence.
* At the time of leaving Leyton Green, for whatever reason, employees or individuals conducting work on behalf of Leyton Green are required to return all property, documentation or any other information related to Leyton Green and, if requested, confirm compliance of the same in writing. In addition, Leyton Green reserves the right to request such information to be returned during the period of notice should Leyton Green Senior Management and / or Owners deem it possible that there could be a risk, intentional or otherwise, of confidentially sensitive information being made available to other parties.