Castlethorpe Community Space CIC
Data Protection Policy

Castlethorpe Community Space CIC ('the Company') recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 which regulates the use of personal data. This does not have to be sensitive data; it can be as little as a name and address.

General Data Protection Regulations (GDPR)

GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. GDPR applies to anyone holding personal information about people, electronically or on paper. The Company has also notified the Information Commissioner that it holds personal data about individuals.

When dealing with personal data, the Company will ensure that:

Data is processed fairly, lawfully and in a transparent manner. This means that personal information should only be collected from individuals if staff have been open and honest about why they want the personal information.

Data is processed for specified purposes only This means that data is collected for specific, explicit and legitimate purposes only.

Data is relevant to what it is needed for. Data will be monitored so that too much or too little is not kept; only data that is needed should be held.

Data is accurate and kept up to date and is not kept longer than it is needed. Personal data should be accurate, if it is not it should be corrected. Data no longer needed will be shredded or securely disposed of.

Data is processed in accordance with the rights of individuals. Individuals must be informed, upon request, of all the personal information held about them.

Data is kept securely. There should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Data Protection

Data Protection applies to all forms of data retained by persons conducting business on behalf of the Company. They are referenced as 'authorised persons' and are principally the Company Secretary and the Directors. Forms of data include paper as well as electronic documents. 'Deletion' of paper based personal data means destruction such as shredding or burning.

Authorised persons may retain names, email and physical addresses and phone numbers of Members who have corresponded with them in addition to the subject matter. Members may request deletion of such information when the matter has been closed for 12 months unless there is a statutory reason that the data has to be retained. This is regarded as personal data.

Persons belonging to organisations that have a business connection to the Company or a Director may have their names, business addresses and phone numbers retained indefinitely while they belong to that organisation. If the person leaves the organisation, they may request their data is deleted. However, they should be aware that there may be statutory reasons why information has to be retained. For example, if there has been a financial transaction, the data has, by law, to be retained for 7 years.

Authorised persons will only use personal data in connection with Company business.

The Company and authorised persons will not use personal data for marketing purposes nor otherwise disclose or share personal data to third pares.

Electronic Security

The Company will adopt appropriate measures to protect the security of its data.

The Company Secretary will have authority to administer security measures including, if necessary as part of an audit, lawful request or complaint, to inspect an email and document account, report on it and require such changes as deemed necessary to ensure the Company's compliance with GDPR. If required changes are not made, the Company Secretary will report it to Company.

When sending emails to a distribution list, personal data (i.e. email addresses) will be bcc'd unless the recipients have effectively consented to their personal data being shared by, for example, having previously written to the authorised person with other recipients copied in explicitly.

When forwarding emails, care will be taken by an authorised person that no personal data is displayed in the forwarded email. This might include the name of a person making a complaint about a service. Generally, long email trails should not be forwarded.

Should a data breach occur, the Company Secretary has authority and responsibility to report it directly to the ICO in accordance with the Law. The Company Secretary will inform the Company of the breach as soon as is possible. Should the Company Secretary not be available, then, in order of availability, the following persons will contact the ICO being the Chair or any other Director.

Subject Access Requests (SARs)

The Company is aware that people have the right to access any personal information that is held about them. Subject Access Requests (SARs) must be submitted in wring in hard copy or by email. If a person requests to see any data that is being held about them, the SAR response must detail:

How and to what purpose personal data is processed

The period the Company tend to process it for

Anyone who has access to the personal data

The response must be sent within 30 days and be free of charge unless, exceptionally, the Company receives so many requests from an individual that they are vexatious.

If a SAR includes personal data of other individuals, the Company must not disclose the personal information of the other individual. That individual's personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the Subject.

Individuals have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restriction of processing of the data and the right to object to data processing, although rules do apply to those requests.

Confidentiality

Authorised persons must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.