# DATA PROTECTION POLICY

**Introduction**

In the course of the Association’s work with our Members we the members of the Board of Directors of The Clifton Moor Business Association (“The Company”) are likely to collect/potentially collect, use, transfer or store personal information about Members, Companies, Employees, Clients, Customers and Suppliers, for example their names and home addresses etc.

This information will not be sold or passed to any other third party without the express written permission of the Member/Individual etc. The data held will be used to contact Members in respect of Membership matters.

The UK’s data protection legislation, including the General Data Protection Regulations (GDPR) contains strict principles and legal conditions which must be followed before and during any processing of any personal information.

The purpose of this policy is to ensure that you, the Member, is aware that the Board has a responsibility to comply with the principles and legal conditions provided by the data protection legislation, including the GDPR and failure to meet those responsibilities are likely to lead to serious consequences.

Firstly, a serious breach of data protection is likely to be a disciplinary offence and will be dealt with under the Company’s disciplinary procedure.

If we access any special categories of personal data without authority, this will constitute a gross misconduct offence. Additionally, if we knowingly or recklessly disclose personal data in breach of the data protection legislation, including the GDPR we may be held personally criminally accountable for any such breach.

Breach of the data protection legislation, including the GDPR rules can cause distress to the individuals affected by the breach and is likely to leave the Company at risk of serious financial consequences.

If there is any doubt about what can or cannot be disclosed and to whom, do not disclose the personal information until you have sought further advice fromthe Company’s Data Protection Officer- Adrian McClaren (Director)

**Definitions**

Data Subject: a living individual.

Data Controller: the person or organisation that determines the means and the purpose of processing the personal data.

Data Protection Legislation: includes (i) the Data Protection Act 1998, until the effective date of its repeal (ii) the General Data Protection Regulation ((EU) 2016/679) **(GDPR)** and any national implementing laws, regulations and secondary legislation, for so long as the GDPR is effective in the UK, and (iii) any successor and supplemental legislation to the Data Protection Act 1998 and the GDPR, in particular the Data Protection Bill 2017-2019 and the E-Privacy Directive (and its proposed replacement), once it becomes law.

Personal data: is any information that relates to an identified or identifiable living individual (data subject) either directly or indirectly. This also includes special categories of personal data. Personal data does not include data which is entirely anonymous or the identity has been permanently removed making it impossible to link back to the data subject.

Processing: is any activity relating to personal data which can include collecting, recording, storing, amending, disclosing, transferring, retrieving, using or destruction.

Special categories of personal data: this includes any personal data which reveals a data subject’s, ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation.

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

**What are the GDPR principles?**

We are a data controller. This means that we are required by law to ensure that we process personal data and special categories of personal data in accordance with the Data Protection Legislation, including the GDPR principles. In brief, the principles provide that:

* Personal data must be processed in a lawful, fair and transparent way.
* The purpose for which the personal information is collected must be specific, explicit and legitimate (and not further processed in a manner incompatible with those purposes).
* The collected personal data must be adequate, relevant and limited to what is necessary for the identified purpose.
* The information must be accurate and, where necessary, kept up to date. Personal data which is inaccurate, having regard for the purpose for which it is processed should be erased or rectified without delay.
* The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.
* The personal data must be kept confidential and secure, and only processed in a way which ensures the appropriate security of the personal data and protection of unauthorised or unlawful processing.

**Other rules under the GDPR state that:**

* The transfer of personal data to a country or organisation outside the EEA should only take place if appropriate measures are in place to protect the security of that data.
* The data subject must be permitted to exercise their rights in relation to their personal data.

The Company and all employees must comply with these principles and rules at all times in their information-handling practices. We are committed to ensuring that these principles and rules are followed, as we take the security and protection of data very seriously.

You must inform us immediately if you become aware that any of these principles or rules have been breached or are likely to be breached.

**What are the lawful reasons under which we would expect to process personal data?**

Whilst carrying out our working activities we are likely to process personal data. The Company will only process personal data where we have a lawful basis (or bases) to process that information. The lawful basis may be any one of the following reasons or a combination of:

1. Consent has been obtained from the data subject to process their personal data for the specified purposes.
2. Where it is necessary to perform the contract we have entered into with the data subject or in order to take steps at the request of the data subject prior to entering into the contract
3. Where we need to comply with a legal obligation.
4. Where it is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the data subject do not override those interests.

There are other rare occasions where we may need to process the data subjects personal information, these include:

1. Where we need to protect the data subject’s interests (or someone else’s interests).
2. Where it is needed in the public interest [or for official purposes].

We must always ensure that we keep a documentary inventory of the legal basis (or bases) which is being relied on in respect of each processing activity which we perform.

**Privacy Notices**

* Personal data must be processed in a lawful, fair and transparent way.

Before we begin collecting or processing personal data directly from a data subject we must ensure that an appropriate privacy notice has been issued to the data subject. The content of the privacy notice must provide in clear and plain language accurate, transparent and unambiguous details of the lawful and fair reason for why we are processing the data. It must provide details of the categories of personal data being obtained and explain how, when and for how long we propose to retain the data subjects personal information. We need to include information around the data subjects’ rights and most importantly, the notice should also explain how we will keep the information secure and protected against unauthorised use.

Where we intend to collect data indirectly from a third party or a public source (i.e. electoral register), we must ensure that a privacy notice is issued to the data subject within a reasonable of period of obtaining the personal data and no later than one month; if the data is used to communicate with the individual, at the latest, when the first communication takes place; or if disclosure to someone else is envisaged, at the latest, when the data is disclosed.

We must only use data collected indirectly if we have evidence that it has been collected in accordance with the GDPR principles.

In all circumstances we must check that we are using an up to date version of the Company’s privacy notice and it is being used in accordance with the Company’s guidelines.

**Purpose Limitation**

* The purpose for which the personal information is collected must be specific, explicit and legitimate.

When we collect personal information we will set out in the privacy notice how that information will be used. If it becomes necessary to use that information for a reason other than the reason which we have previously identified we must usually stop processing that information. However, in limited circumstances we can continue to process the information provided that our new reason for processing the personal information remains compatible with our original lawful purpose (unless our original lawful basis was consent).

**Adequate and relevant**

* The collected personal data must be adequate, relevant and limited to what is necessary to meet the identified purpose.

We must not collect, store or use unnecessary personal data and we must ensure that personal data is deleted, erased or removed within the Company’s retention guidelines.

The Company will review its records and files on a regular basis to ensure they do not contain a backlog of out-of-date or irrelevant information and to check there are lawful reasons requiring information to continue to be held.

**Accurate and kept up to date**

* The information must be accurate and kept up to date.

**Kept for longer than is necessary**

* The personal data should not be kept any longer than is necessary for the purposes for which it is to be used.

Different categories of personal data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a particular period of time will be destroyed in accordance with its retention of data policy.

**Kept confidential and secure**

* The personal data must be kept confidential and secure and only processed by authorised personnel.

**To achieve this we must follow these steps:**

* The Company has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data. These procedures must always be adhered to and not overridden or ignored.
* Where the Company provides code words or passwords to be used before releasing personal information, for example by telephone, we must strictly follow the Company’s 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.
* Ensure that any personal data which we hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
* We do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which would be inappropriate to share with that data subject.
* We do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable us to carry out our duties and has been authorised by a Member of the Board.
* Ensure that when working on personal information as part of our duties when away from your workplace and with the authorisation of a Board Member, we continue to observe the terms of this policy and the Data Protection Legislation, in particular in matters of data security.
* Ensure that hard copy personal information is disposed of securely, for example cross-shredded.
* Manual personnel files and data subject files are confidential and are stored with a Member of the Board in locked filing cabinets. Only an authorised Board Member has access to these files. For a list of authorised Board Members, please contact Adrian McClaren. These will not be removed from their normal place of storage without good reason.
* Data stored on memory sticks, discs, portable hard drives or other removable storage media is kept in locked filing cabinets.
* Data held on computers are stored confidentially by means of password protection, encryption and/or coding.
* The Company has network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed.

**Transfer to another country**

* Transfer of personal data to countries or organisations outside of the EEA should only take place if appropriate measures are in place to protect the security of that data.

We do not generally have a need to transfer data outside of the European Economic Area (EEA). However, if we are requested to transfer personal data to a country or organisation outside of the EEA we must not transfer personal data to a country or organisation unless that country or organisation ensures an adequate level of protection in relation to the processing of personal data and we have in place safeguards to ensure this is done. We must speak to you before we send personal data outside of the EEA.

**The data subject rights**

* The data subject must be permitted to exercise their rights in relation to their personal data.

Under the GDPR, subject to certain legal limitations, data subjects have the right to be informed about the collection and use of their personal data. They have a number of legal rights regarding how their personal data is processed. At any time a data subject can request that the Company should take any of the following actions, subject to certain legal limitations, with regard to their personal data:

* Allow access to the personal data
* Request corrections to be made to personal data
* Request erasure of data
* Object to the processing of data
* Request that processing restrictions be put in place
* Request a transfer of personal data
* Object to the processing of personal data in certain circumstances
* Right to be notified of a data security breach

***There are different rules and timeframes that apply to each of these rights. We must follow the Company’s policies and procedures whenever we process or receive a request in relation to any of the above rights.***

**How should we respond to a data subject request?**

We must follow the Company’s data subject access procedure which details how to deal with requests and it describes the circumstances where a fee may be charged. The procedure includes the following:

* We always verify the identity of the person making a data subject request and the legitimacy of the request.
* If we are unsure as to whether we are authorised to action the request we check the privacy notice to ascertain who is authorised to deal with data subject requests. If we are still unsure how to handle the request we would forward the request to Elizabeth Lebeter Chairperson and Director for clarification.
* If we are authorised to deal with the request, we do not give out confidential personal information unless we have received the appropriate consent from the data subject. We will seek explicit written consent to process the data subject request and ensure that we keep a clear audit trail of the request and our response.
* **WE DO NOT SHARE personal data with a third party, unless the data subject has given their explicit prior consent to the sharing of their information. A third party is anyone who is not the actual data subject and can include a family member of the data subject.**
* We will take great care not to accidentally share information with an unauthorised third party.

We are aware that those seeking information sometimes use deception in order to gain access to it. We will take all reasonable steps to ascertain clarity prior to the release of any data. If we remain in doubt no information will be released.

**Categories of information**

During the course of our business we may be required to process personal data which falls into different categories, general personal data and special categories of personal data. All data would be processed in accordance with the privacy notice and at all times in a confidential manner. However, where that data is classed as a special category extra care would be taken to ensure the privacy and security of that data. This means that we would maintain a high level of security and we would only share this data with those who are also authorised to process that data.

**When will we need to seek consent?**

In limited circumstances during our work we may need consent from a data subject in order to process personal data or special categories of data. We will ensure that we are provided with training and details of which circumstances consent is needed and the type of consent that should be sought.

However, in limited circumstances, we may find it necessary to request a data subject to provide written consent to allow the processing of special categories of personal data. We will ensure that we are provided with training and details of which circumstances consent is needed and the type of consent that should be sought. If it becomes necessary to request consent to process special categories of personal data, we must provide the data subject with details of the information that will be required and why it is needed, so that they can make an informed decision as to whether they wish to provide consent.

We must not compel a data subject to provide written consent. Giving consent will always be a decision made by freewill and choice and is not a contractual condition. Consent can be withdrawn at any time without any reason provided. We must not subject a data subject to a sanction or detriment as a consequence of withdrawing consent. This would be viewed a serious disciplinary issue.

**Action to be taken in the event of a data protection breach**

A data breach will arise whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on a data subject.

In the event of a security incident or breach, we must follow the Company’s Data Breach Policy which includes immediately informing the Data Protection Officer so that steps can be taken to:

* Contain the breach;
* Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
* To limit the scope of the breach by taking steps to mitigate the effects of the breach.

The Data Protection Officer will determine within 72 hours the seriousness of the breach and if the Information Commissioner’s Office (ICO) and/or data subjects need to be notified of the breach.

**Record keeping**

* Clear records will be kept at all times of our activities in relation to data processing, data sharing and retention.

**Training**

All Company personnel that handle personal data must have a basic understanding of the Data Protection Legislation, including the GDPR. Personnel with duties such as computer and internet security, marketing and database management may need specialist training to make them aware of particular data protection requirements in their specialist area.

We will provide continuous training and updates on how to process personal data in a secure and confidential manner and in accordance with the spirit of the Data Protection Legislation, including the GDPR. We are required to attend all training and to keep ourselves informed and aware of any changes made to privacy notices, consent procedures and any other policies and procedures associated with our internal processing of personal data.

We must regularly review our processing activities and ensure that we are acting in accordance with the most current best practice and legal obligations in relation to data security and confidentiality.

**Automated processing and decision making**

From time to time we may use computer programmes to process data and make automated decisions. We will provide a separate notice explaining when and how this happens. Where automated processing or decision making does take place and the effect of that processing impacts on the freedoms and legitimate interests of the data subject, then in certain circumstances the data subject can request for human intervention. This means that they can ask for a human to review the machine made outcome/decision.

**Sharing personal data**

We may share personal data internally as is necessary. We must always ensure that personal data is only shared with authorised persons and is shared in accordance with the purposes stated in any privacy notice or consents. Extra care and security would be taken when sharing special categories of data or transferring data outside of the Company to a third party.

**Direct Marketing**

We are subject to specific rules under the GDPR in relation to marketing our services. Data subjects have the right to reject direct marketing and we must ensure that data subjects are given this option at first point of contact. When a data subject exercises their right to reject marketing we must desist immediately from sending further communications.

**Complaints**

If a member believes that this policy has been breached or to exercise all relevant rights, queries or complaints please in the first instance contact a Member of the Board initially.

**Changes to this policy**

We reserve the right to change this policy at any time so please always check this document regularly to ensure we are following the correct procedures.

This policy was last updated on 1 June 2019

**Compliance with GDPR is everyone’s responsibility.**

By signing this policy you confirm that you have read and understood the content of this policy.