BRAND VISTA | Customer Experience Alignment

The Heath Business and Technical Park, Runcorn, WA7 4QX
T 0800 334 5425 **E** enquiries@brand-vista.com
Support Team **T** +44 (0) 1928 736 620 brand-vista.com

Brand Vista Limited - Data Protection Policy (including GDPR May 2018)

1. Policy Statement

Brand Vista Limited is committed to a policy of protecting the rights and privacy of individuals in accordance with The Data Protection Act 2018 and the GDPR requirements 25th May 2018. The policy applies to all staff at Brand Vista Limited.

As a matter of good practice, other organisations and individuals working with Brand Vista, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that any staff who deal with external organisations will take responsibility for ensuring that such organisations sign a contract agreeing to abide by this policy.

2. Legal Requirements

Data are protected by the Data Protection Act 2018, which came into effect on 23rd May 2018 and GDPR 25th May 2018. Its purpose is to protect the rights and privacy of individuals and to ensure that personal data are not processed without their knowledge, and, wherever possible, is processed without their consent.

The Act and the Regulations require us to register the fact that we hold personal data and to acknowledge the right of 'subject access' – voluntary and community group members and staff must have the right to copies of their own data.

3. Managing Data Protection

We will ensure that our details are registered with the Information Commissioner's Office. Current registration expires 1st September 2019.

4. Purpose of data held by Brand Vista Limited

Data may be held by us for the following purposes:

1. Staff Administration
2. Provision of services to clients
3. Accounts & Records
4. Advertising, Marketing & Public Relations
5. Information and Databank Administration
6. Research

5. Data Protection Principles

In terms of the Data Protection Act 2018 in some instances, we are the 'data controller', and as such determine the purpose for which, and the manner in which, any personal data are, or are to be, processed. We must ensure that we have:

5.1. Fairly and lawfully processed personal data

We will always put our logo on all paperwork, stating their intentions on processing the data and state if, and to whom, we intend to give the personal data. Also provide an indication of the duration the data will be kept.

5.2. Processed for limited purpose

We will not use data for a purpose other than those agreed by data subjects (client and supplier staff and others). If the data held by us are requested by external organisations for any reason, this will only be passed if data subjects agree. Also external organisations must state the purpose of processing, agree not to copy the data for further use and sign a contract agreeing to abide by The Data Protection Act 2018 and Brand Vista's Data Protection Policy.

5.3. Adequate, relevant and not excessive

Brand Vista Limited will monitor the data held for our purposes, ensuring we hold neither too much nor too little data in respect of the individuals about whom the data are held. If data given or obtained are excessive for such purpose, they will be immediately deleted or destroyed.

5.4. Accurate and up-to-date

We will provide our members with a copy of their data once a year for information and updating where relevant. All amendments will be made immediately and data no longer required will be deleted or destroyed. It is the responsibility of individuals and organisations to ensure the data held by us are accurate and up-to-date. Completion of an appropriate form (provided by us) will be taken as an indication that the data contained are accurate. Individuals should notify us of any changes, to enable personnel records to be updated accordingly. It is the responsibility of Brand Vista Limited to act upon notification of changes to data, amending them where relevant.

5.5. Not kept longer than necessary

We discourage the retention of data for longer than it is required. All personal data will be deleted or destroyed by us after one year of non-membership has elapsed.

5.6. Processed in accordance with the individual's rights

All individuals that Brand Vista Limited hold data on have the right to:

- Be informed upon the request of all the information held about them within one month (subject access requirements GDPR).
- Prevent the processing of their data for the purpose of direct marketing.
- Compensation if they can show that they have been caused damage by any contravention of the Act.
- The removal and correction of any inaccurate data about them.

5.7. Secure

Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

All Brand Vista Limited computers have a log in system and our Contact Database is password protected, which allow only authorised staff to access personal data. Passwords on all computers are changed frequently. All personal and financial data is retained by the Chief Finance Officer on a personal laptop in a file which is not accessible to others. When staff members are using the laptop computers out of the office care should always be taken to ensure that personal data on screen is not visible to strangers.

5.8. Not transferred to countries outside the European Economic Area, unless the country has adequate protection for the individual

Data must not be transferred to countries outside the European Economic Area without the explicit consent of the individual. Brand Vista Limited takes particular care to be aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the European Economic Area.

6. Client Specific Data

Appendix A: Specific requirements for a client (example Client A.)

1. **Data Management**

All information whether held electronically or in physical form will be held only by staff assigned to the Client A. contract.

The issue of data to staff will be controlled by the Account Director who will maintain a log showing updates, changes, circulation and destruction dates. Where required by the client, electronic data will be encrypted and password controlled and physical data will be stored in a locked cabinet.
Electronic data transferred between Client A. and Brand Vista or vice versa will be encrypted and password controlled where agreed as necessary between both parties.

2. **Data Destruction**

At Client A's direction all confidential information will be destroyed. In any case this information will be destroyed at the end of the contract.
Paper and shreddable material;
This media will be destroyed using a shredding technique such that Confidential Information in this media will be completely destroyed. This will be carried out by an approved 3rd party specialist. BV will supervise this activity.
Electronic Media;
This media will be wiped using a Client A. approved wipe or degaussing tool. This activity will be sub-contracted to Urban IT, BV's IT sub-contractor. Urban IT will be informed of the necessity of meeting Client A. standards and requirements.

Certification;
The specific processes and methods used will be documented by the Account Director and records of where and when Confidential Information has been destroyed. These records will be available to Client A. upon demand.

3. Third Party Management

The Client A. data management requirements have been relayed to the 3rd party supplier (Mustard Research). Mustard control data in accordance with their DATA/IT RISK ASSESSMENT AND SECURITY POLICY – April V3. Monthly meetings are held with Mustard to ensure compliance with data protection requirements.

4. Storage

Brand Vista data should not be stored on computers or portable media devices unless access is required when network connectivity is not available. When it is necessary, data should only be stored on authorised devices.

Encryption is applied to all authorised data storage devices attached to desktop, laptop or tablet computers. In certain cases, it may not be feasible for certain devices to be encrypted and each exception to a device will be given full and careful consideration as to its use and any decision made will be based on best practice and business need.

Where exceptions have been identified for not encrypting specific devices, computer policy settings (enforced at domain level) which enable/disable encryption can be applied individually to a specified computer and/or groups of computers.

When a portable, Brand Vista recommended, data storage device is used, the instructions for the correct use must be followed to ensure the data is encrypted. Personal storage media and equipment must not be connected to the Brand Vista network and must not be used to store Brand Vista data.

Other portable USB devices include mobile phones, cameras, PDAs etc. These other devices should not be used to store Brand Vista data. You must contact the Account Manager if you need to use these devices as part of your job.

On encryption of an authorised portable storage device (e.g. USB data stick) the user will need to set a password for accessing the device. The password for encrypted portable devices will be a combination of 8 alphanumeric characters - fully enforced at the domain level. Using the portable device on any other computer after being encrypted will require a password in order to access it.

Brand Vista employees and associates have an explicit responsibility to ensure:

- No one other than authorised person/s are aware of the encryption/decryption password for the device, media or system.
- Any portable device or media is not given to any unauthorised persons for safe keeping.
- Any portable device or media is not left discarded or unattended in a public place.

8th April 2019

John K. Carson
CFO