Drunch needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled, and stored to meet the company's data protection standards – and to comply with the law.
WHY? This data protection policy ensures Drunch:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers, and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

DATA PROTECTION LAW:
The Data Protection Act 1998 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or elsewhere. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.
The Data Protection Act is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific and lawful purposes
- Be adequate, relevant, and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of the data subjects
- Be protected in appropriate ways
- Not be transferred outside of the EEA, unless that country or territory also ensures an adequate level of protection.

PEOPLE, RISKS, RESPONSIBILITIES:

- This policy applies to Drunch including all branches of Drunch.
- All contractors, suppliers and other people working on behalf of Drunch. It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:
- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

DATA PROTECTION RISKS:
This policy helps you to protect Drunch from some very real data security risks including:

- Breaches of confidentiality. For instance, information being given out inappropriately
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them such as reputional damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

RESPONSIBILITIES:

- Everyone who works for or with Drunch has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility
- The Directors are ultimately responsible for ensuring that Drunch meets its legal obligations. The Marketing Manager is responsible for:
- Keeping the Directors updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data that Drunch holds about them (also known as a 'subject access request')
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data The Directors are also responsible for
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services the company is considering using to store or process data i.e. cloud computing services.
- Approving any data statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets like newspapers
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

GENERAL GUIDANCE

- The only people able to access data covered by this policy should be those who need it for their work. Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Drunch will provide training to all employees to help them understand their responsibilities when handling data Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of appropriately. Employees should request help from their line manager or Director if they are unsure about any aspect of data protection.

DATA STORAGE:

These rules describe how and where data should be safely stored.
Questions about storing data safely can be directed to a Director or Marketing Manager.
When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it; these guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

When not required, the paper or files should be kept in a locked draw or filing cabinet. Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer. Data printouts should be shredded and disposed of securely when no longer required. When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts. Data should be protected by strong passwords that are changed regularly and never shared between employees. If data is stored on removable media, these should be kept locked away securely when not being used. Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service. Servers containing personal data should be sited in a secure location, away from general office space and data should be backed up frequently. Those backups should be tested regularly. Data should never be saved directly to laptops or other mobile devices like tablets or smart phones. All servers and computers containing data should be protected by an approved security software and firewall.

DATA USE:

Personal data is of no value to Drunch unless the business can make use of it.
However, it is when personal data is access and used that it can be at the greatest risk of loss, corruption, or theft. When working with personal data, employees should ensure the screens of their computers are always locked when left unattended. Personal data should not be shared informally. Seriously consider the safety of email when communicating personal information as it is not considered as secure.

- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the EEA
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

DATA ACCURACY:

The law requires Drunch to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort the business should put in to securing its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets. Staff should take every opportunity to ensure data is updated i.e. confirming a customer's details when they call. We will make it easy for data subjects to update the information we hold about them. Data should be updated as inaccuracies are discovered. I.e. if a customer can no longer be reached on their stored telephone number, it should be removed from the database. It is the Studio Manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

SUBJECT ACCESS REQUESTS:

All individuals who are the subject of personal data held by the company are entitled to ask what information the company holds about them and why or how to gain access to it.
Be informed how the company is meeting its data protection obligations. If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the info@drunch.co.uk and we will aim to provide the relevant data within 14 days. Drunch will always verify the identity of anyone making a subject access request before handing over any information.

DISCLOSING DATA – OTHER REASONS:

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Drunch will disclose requested data. However, Drunch will ensure the request is legitimate, seeking assistance from the Directors and a legal advisor where necessary.

PROVIDING OTHER INFORMATION:

Drunch aims to ensure that individuals are aware that their data is being processed, and that they understand

- How the data is being used
- How to exercise their rights To these ends the company has a privacy statement, setting out how data relating to individuals is used by the company

PRIVACY STATEMENT:

Preservation of your privacy is important to Drunch and we are committed to letting you know how we use your personal information and to making only responsible use of your data. References to "we", "us", "you" or "our" in this Privacy Statement are references to Drunch, a company limited in England and Wales.

1) Information about you We will collect personal information from you when you or your organisation enquire about our activities, register as a member with us or subscribe to one of our services. This may include your name, title, email address, physical address, telephone numbers and job title. We may also ask for some additional, non-personal information.

2) Our use of this information Your personal information will only be used to process your requests, to provide you with our services, and to provide you with information relating to our services and all other services which we think you may be interested in.

3) Security We will take reasonable precautions to prevent the loss, misuse, or alteration of information you give us. Communications in connection with this service may be sent by e-mail. For ease of use and compatibility, communications (other than payments where applicable) will not be sent in an encrypted form unless you require it and provide the certification to enable us to communicate with you in that way. E-mail unless encrypted is not a fully secure means of communication. Whilst we endeavour to keep our systems and communications protected against viruses and other harmful effects we cannot bear responsibility for all communications being virus-free. 4) Cookies If cookies are used they will only be used to assist the purposes set out in this Privacy Statement, but cookies will not be used if we do not consider them to be necessary.

5) Other information If you would like us to correct or update any information, or if you would like information deleted from our records, then please email us at info@drunch.co.uk

This privacy policy may be updated from time to time, so please check it periodically.

Links within our sites to other websites are not covered by this privacy policy