Data Protection Policy

Human Resources
Data Protection Policy

Aims of the Policy

apetito is committed to meeting its obligations under data protection law. As a business, apetito handles a range of Personal Data relating to its customers, staff and others. Personal Data includes information identifying living individuals kept as written records (both paper-based and electronic) and in other formats, such as CCTV recordings. (Please see the "What is Personal Data" section of this policy for more details).

Collection and processing of Personal Data is subject to a variety of legal requirements. It is the responsibility of apetito to demonstrate how it complies with these legal requirements and that it has procedures in place to handle personal information securely and appropriately. It is vital that apetito operates to a very high standard. Failure to do so can have serious commercial and legal implications for apetito's business.

By law, apetito must comply with the eight data protection principles. These are set out in the Data Protection Act of 1998 ("DPA"), which in summary, require that Personal Data must be:

Principle 1: processed fairly and lawfully

Principle 2: processed for limited purposes

Principle 3: adequate, relevant and not excessive

Principle 4: accurate and up to date

Principle 5: not kept longer than necessary for the purpose

Principle 6: processed in accordance with the data subject's rights

Principle 7: secure

Principle 8: not transferred to countries outside the EEA without adequate protection

What do I need to know?

This policy is intended to provide an overall framework for apetito to demonstrate its compliance with data protection law. It contains explanations of apetito's legal requirements under the DPA and the operational procedures in place at apetito, including:

- Roles and Responsibilities
- The Legal Context
- Notification with the Information Commissioner’s Office
- Data Storage
- Access to Data
- Data Security
- Data Destruction
- Handling Breaches of Data Protection
- Maintaining Compliance

All staff (permanent or temporary) should make sure they are familiar with the content of this policy and comply at all times with the procedures set out in this policy when handling Personal Data.

Also included within this policy are Data Protection and Privacy Statements for employees and applicants, in which apetito states to its employees and job applicants the purposes for which

Personal Data collected about them will be used and the circumstances in which such data will be disclosed.

Who does this policy apply to?

This policy applies to all users of Personal Data, that is:

- All entities of apetito Limited (including related companies if appropriate, including all sites at which the apetito operates now or at any time in the future;
- All managers, i.e. line and business managers, as well as those in the HR department who use Personal Data; and
- All employees (whether permanent, temporary or contractors) who use Personal Data.

Under the terms of their contract with apetito all employees, temporary workers and others who have authorised access to Personal Data are responsible for handling Personal Data and maintaining confidentiality appropriately at all times.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

Failure by any of these parties to adhere to this policy may result in civil or criminal legal action being taken against apetito, or against individual managers or employees by data protection authorities, or by the individuals to whom the Personal Data relates.

It is the responsibility of apetito to ensure that its staff are aware of and comply with this policy. Any breach of this policy will be taken very seriously and employees who act outside the requirements or guidance set out in this policy will be asked to explain the reasons for their actions and may face disciplinary action. Wilful and negligent non-adherence to this policy by any employee is a serious disciplinary matter which could result in dismissal.

Responsibilities of apetito

To enable it to meet its obligations under data protection law, apetito will provide the following:

- Training for apetito managers (and relevant employees) on data protection issues and apetito procedures;
- Information for employees on data protection issues and apetito procedures as part of induction and on-going employment;
- Appropriate procedures to safeguard Personal Data and to ensure compliance with the eight data protection principles; and
- An escalation process whereby any potential issues should be raised with the Financial Director or, in their absence the HR Director.

  Any questions or concerns about the operation of this policy and/or the handling of Personal Data should be referred in the first instance to the Financial Director or in their absence the HR Director.

The Legal Context

What is Personal Data?

Personal Data - is any information:

- from which a living individual can be identified or which, together with other information that apetito possesses (or is likely to possess) an individual can be identified; and
- is processed, or intended to be processed by electronic or manual means, as part of a 'relevant filing system'.

Processing - is any activity that involves use of the Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

For apetito this applies to: Personal Data and employment records relating to current, past and prospective employees and Personal Data of customers placing an order for an apetito product.

Sensitive Personal Data - is a special category of Personal Data consisting of information about a living individual as to: racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, the commission or alleged commission of an offence, or any proceedings for any offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of any court in such proceedings

apetito collects some items of Sensitive Personal Data. For example:

- a specific dietary or medical requirement of a customer in relation to the processing of their order of an apetito product; or
- an employment law requirement in relation to apetito staff (such as equal opportunities monitoring purposes, or for health and safety reasons).

The collection and processing of Sensitive Personal Data is strictly regulated, generally requiring the explicit informed consent of the data subject to collect and process it (unless the collection is a legally imposed obligation) and imposing severe restrictions on access.

It is apetito's policy to collect Sensitive Personal Data only when absolutely necessary.

Sensitive Personal Data must be made available to users only on a strict "need to know" basis and managed with the highest practical level of security and confidentiality. Sensitive Personal Data should only be gathered from individuals if it is essential, in which case any necessary consent should be obtained.

Fair and lawful processing

The DPA is intended to ensure that Personal Data is processed fairly and without adversely affecting the rights of the data subject. The data subject must be told who the Data Controller is, the purpose for which the data is to be processed and the identities of anyone to whom the data may be disclosed or transferred.

For Personal Data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the Data Controller or the party to whom the data is disclosed. When Sensitive Personal Data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Processing for specified lawful purposes

Personal Data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the DPA. This means that Personal Data must not be collected for one purpose and then used for another.

If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Notification with the Information Commissioner's Office

apetito is required to notify the Information Commissioner's Office ("ICO") that it handles Personal Data. Notification is the process by which a "Data Controller" (i.e. the organisation that determines the purposes of the processing of Personal Data) gives the ICO details about its processing of personal information. This notification includes: the types of information collated, the purpose for which it is used, and to whom information may be disclosed.

Notification is a statutory requirement and failure to notify with the ICO is a criminal offence. The full procedure for notification can be found at: www.ico.gov.uk. The main requirements set out by the ICO are as follows:

- one notification is required for each legal entity that is a Data Controller
- apetito must renew its notification(s) annually
- apetito must also notify the ICO when any part of its entry changes, or becomes inaccurate or incomplete within 28 days of such a change taking place.

The ICO keeps a register of all Data Controllers, which is available to the public for inspection. This contains: name and address of Data Controller, general description of the processing of personal information.

apetito's Data Controller has responsibility for maintaining its notification as a Data Controller with the ICO.

Data Storage

Personal Data should only be collected to the extent that it is required for the specific purpose notified to the data subject and must be accurate and kept up to date at all times. All employees, temporary workers and others at apetito handling Personal Data must follow the general data storage rules set out in this section.

Paper records

- Paper records containing Personal Data must always be stored securely unless in use and should not be left on desks or other areas accessible by third parties. Cabinets containing files must be kept locked and offices in which cabinets are located should also be locked when not in use.
- Documents containing Personal Data whose loss could be detrimental to apetito or its employees, or customers should be marked: [***"Confidential – For Internal Use only"*** and should be circulated to relevant individuals internally in a sealed envelope marked: ***"To be opened by Addressee only"***.

Electronic records

- Electronic records containing Personal Data:
  - must either be encrypted or must be kept on devices which have their hard drives encrypted;
  - must be kept in separate folders to electronic files not containing Personal Data;
  - must only be transferred from desktop computers to portable devices if absolutely necessary. Records may only be put onto portable devices or media such as CDs, USB memory sticks or laptops if the device itself and/or the records are encrypted.
- Desktop computers and laptops on which electronic records are stored or accessed must be running an up-to-date operating system and up-to-date firewall and anti-virus software.
- If the premises where paper records and computer equipment and devices containing electronic records are kept are alarmed then the alarm must always be set.

apetito has a separate policy on CCTV available via the apetito intranet

Access to Data

Processing in line with data subject's rights

Data must be processed in line with the data subjects' rights. Data subjects have a right to:

- request access to any data held about them by a Data Controller;
- prevent the processing of their data for direct-marketing purposes;
- ask to have inaccurate data amended; and
- prevent processing that is likely to cause damage or distress to themselves or anyone else.

Requests by Individuals relating to their own Personal Information

Under the DPA, individuals have the right to request Personal Data (in any format) held about them by apetito. This is known as a ‘Subject Access Request’.

It is important to note that this right only:

- relates to the requesting individual's Personal Data (and not to information relating to other people); and

- allows access to information contained within documents (rather than documents themselves).

  There are some exemptions under the DPA in giving access to certain information contained within files. The main reasons for refusals relate to:

- protecting the health and safety of anyone concerned;
- protecting the privacy of a third party who may be identified if information is shared.

To exercise their right of access, individual data subjects must make their request in writing and give appropriate notice to apetito[1].

[1]NB: if the request is made by a disabled person, apetito may need to make reasonable adjustments to this expectation, as required under the Disability Discrimination Act 1995, for example by accepting a verbal request for information.

Organisations must comply with Subject Access Requests within 40 days and may charge a fee of up to £10 for doing this.

There is no limit under the DPA to the number of requests an individual may make for access to Personal Data held about them. However, organisations are not obliged to respond to similar or identical requests for information which have already been dealt with and without a reasonable lapse of time. The law does not define what constitutes ‘reasonableness’, but expects that organisations consider how often information is updated and how much new information is likely to have been recorded between requests.

Procedure for dealing with Subject Access Requests

Any member of staff who receives a written request for access to Personal Data should forward it immediately to the Head of HR. All Subject Access Requests shall be dealt with in accordance with apetito's “Handling Subject Access Requests Procedure" which is available from the Head of HR or via the apetito intranet.

Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by apetito. In particular they should:

- check the caller's identity to make sure that information is only given to a person who is entitled to it;
- ask that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked;
- refer to their line manager or the Data Protection Officer for assistance in difficult or unusual situations. No-one should be bullied into disclosing personal information; and keep a record of all disclosures.

Data Security

Employees and other individuals who handle Personal Data at apetito are responsible for ensuring they only handle Personal Data in line with the requirements of the Data Protection Act 1998 and this policy. As a general principle, this includes:

- not sharing information with third parties without the consent of the individual concerned; and
- not enabling third parties to access Personal Data through insufficient attentiveness to its storage or management.

apetito must ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The DPA requires apetito to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, as follows:

- **Confidentiality**: only people who are authorised to use the data can access it.
- **Integrity**: Personal Data should be accurate and suitable for the purpose for which it is processed.
- **Availability**: authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on apetito's central computer system instead of individual PCs.

Any keys, passwords, user details, key cards or other security measures used to access data subjects' details are personal to the Head of HR and must not be shared with anyone.

Practical Security Measures

apetito employs several security procedures and technologies to maintain the security of Personal Data. Employees and others at apetito with authorised access to Personal Data must follow these procedures at all times. These include:

- **Entry controls**: reporting any stranger seen in entry-controlled areas.
- **Secure lockable desks and cupboards**: keeping desks and cupboards locked if they hold Personal Data of any kind. (Please see: "Data Storage" section for further information about the storage of Personal Data.)
- **Secure methods of disposal**: shredding paper documents containing Personal Data. Media containing electronic documents should be physically destroyed when they are no longer required. (Please see: "Data Destruction" section for further information about the procedures for destruction of Personal Data.)
    - Equipment: ensuring that individual monitors do not show any form of Personal Data or confidential information to passers-by and that individuals log off from or lock their PC when it is left unattended.

- Passwords / Restriction by User: using passwords (which are regularly updated) and user access to restrict access to documents containing Personal Data.
- On-Site Working: at all times where possible, keeping all files and documents containing Personal Data on-site, or where a specific business need requires off-site working, encrypted memory sticks and password protected access should always be used.
- Strict policies on Subject Access Requests: avoiding accidental disclosure in person, by phone, email or other methods (e.g. when conversations are overhead by others present or by failing to adequately verify the identity of the person making a request for information). (Please see: "Access to Data" section for more detail.)
- Security Software: ensuring that software and internet security are regularly updated.

This list is for guidance and is not exhaustive. Further advice should be sought from the apetito Data Protection Officer where necessary. A risk assessment is also carried out annually as specific security requirements may change over time. (Please see the section: "Maintaining Compliance".)

Disclosure of Personal Data to Third Party Data Processors

It may be necessary to disclose Personal Data where this is:

- to enable apetito to perform its obligations under the contract of employment with the individual; or
- necessary for the conduct of apetito's business; or
- required by law.

If apetito discloses Personal Data to outsourcing companies or third party data processors, whether external organisations or other companies owned by or related to apetito, (for example for payroll processing, telephone marketing, pensions administration, archiving or computer support), additional security measures must be taken, to ensure such third parties handle the Personal Data appropriately.

In such circumstances apetito should ensure the following:

Due Diligence - satisfy itself that the third party Data Processor is reliable, that it will keep data confidential, and that it has adequate technical and organisational security measures in place

- (e.g. this might be by requiring a minimum set of due diligence questions / requirements to be addressed, prior to entering into a contract);
- **Contracts with Third Party** - ensure a contract is in place binding the data processor to the same obligations that apply to apetito, and under which the data processor agrees to act only in accordance with instructions from apetito, and to take appropriate technical and organisational security measures when processing Personal Data; and
- **Consider what is necessary** - at all times ensure that no more Personal Data than necessary is provided by apetito to the third party data processor for the performance of the contract.

Unauthorised disclosure of Personal Data may result in disciplinary proceedings, could be grounds for dismissal and it could also lead to criminal proceedings being taken against anyone who has done so.

If an employee of apetito has any doubt on whether Personal Data may be disclosed or transferred, they should seek the advice of the Financial Director or Head of HR before any transfer is made.

Data Destruction

apetito's approach to data destruction is that files and information relating to customers, and employees will only be destroyed upon specific request from the customer or employee. apetito will use its best efforts to make it clear to customers and employees that should they wish data about them to be destroyed then this will be done in an expeditious manner and securely.

apetito will keep a record of all employee Personal Data destroyed.

- **Paper records** - paper records containing information about data subjects will be placed in confidential waste bins. Paper records should never be placed in normal waste bins, whether shredded or not
- **Electronic records**
    - media which contains electronic records but which is damaged or will not be used again (e.g. CDs) should be physically destroyed
    - electronic records and data files held on computers, laptops, USB sticks or other portable devices should be destroyed

Handling Breaches of Data Protection

A security breach may take place for several reasons, including one or more of the following:

- Loss or theft of Personal Data
- Inappropriate access/unauthorised use of Personal Data
- Equipment failure
- Human error
- Unforeseen circumstances, such as fire or flood
- Hacking or obtaining of information by deception.

It is the responsibility of staff to report to their line manager any actual, potential or suspected breach of data protection law as soon as possible. Managers should then report this to the Financial Director and Head of HR

In considering its response to a potential or actual breach of its data protection obligations, apetito's managerial team should then consider taking the following steps, in the order listed below:

1. Containment and Recovery of Data	This may include: • Initial investigation • Establishing a data recovery plan • Specialist input from IT and legal advisers. The following issues should be considered: • Who needs to lead the investigation • Who should be informed of the breach and any actions that should be taken to contain it (e.g. changing door codes / passwords) • What can be done to recover lost data • Consider whether the Police (other regulatory authorities) need to be informed.
2. Risk Assessment	Consider the seriousness of the risk to individuals arising out of the breach. The following should be taken into account: • Type of data involved (i.e. is does it involve Sensitive Personal Data) • How many people are affected • Who has been affected (e.g. staff, customers) • Level of sensitivity • Risk of harm, damage or distress to the affected data subjects • Who now has access to the Personal Data • The need to inform third parties • Any wider risks (e.g. public health, reputational issues) The level of assessed risk should also inform the timescale for response and whether to notify the affected individuals and / or the ICO that a breach of Personal Data has taken place.

3. Notification [2]	Consider whether notification of the breach is relevant. (NB: This is different to the annual requirement to notify with the ICO referred to earlier in this policy – which is a legal requirement.) The following should be taken into account: • Any legal and contractual requirements to notify • Consider if notifying the individuals who have been affected by the breach will enable them to take steps to protect themselves • If notifying affected individuals is appropriate consider the best means of notification • Is the breach sufficiently serious to be notified to the ICO
4. Evaluation	Establish if the breach is due to a one-off or systemic problem and take appropriate steps to remedy the situation and to prevent it happening again. This is likely to require completion of a new risk assessment and amendments to existing procedure and policy.

Further guidance on this issue should be sought if necessary, for example from the ICO website, www.ico.gov.uk, or from apetito's legal advisors.

[2] In serious cases, breaches should be notified to the ICO. In making an assessment as to whether to notify the ICO, apetito managers should take into account the potential level of harm to individuals, either through the volume of data breached or its sensitivity

Maintaining Compliance

Annual review and Risk Assessment

This data protection policy is subject to an annual review, unless legal changes or other circumstances mean that an interim review is also appropriate. The next review date is set for [March 2014].

Risk Assessments and Policy Review

apetito will carry out an annual risk assessment of data protection issues as part of each annual review and will put in place and / or update procedures to mitigate the impact of any identified risks.

Responsibility for reviewing and updating this policy will rest with the Financial Director and HR Director

Appendix 1

DATA PROTECTION AND PRIVACY STATEMENT – EMPLOYEES

Human Resources
Data Protection Policy

apetito Limited ("the Company) respects the privacy of the personal information you provide as an employees of the Company. This Statement explains how your information will be used and protected. It applies to information held about you now, or at any future date.

Information that may be held about you includes, but it not limited to: your CV; application form; references; appraisal and disciplinary records; salary and pension details; details of other benefits; results of medical, security and financial checks; sickness records; personal contact details; bank account and tax details; and any other information relevant to the following purposes. This information may be held manually or electronically (e.g. databases; processing, communication, payment and other systems). It will be available, as required, at any location in which the Company operates.

The Company may use your personal information for the following purposes:

- to appraise your job performance and make decisions concerning your recruitment, promotion, training, transfer, redeployment or career development;
- to determine, calculate and review your salary, bonuses and any other staff benefits including pension entitlements;
- to process payment of your salary, other authorised expenses or benefits to your account or by any other means;
- to take appropriate action in connection with illness, injury or death while you work;
- to comply with any statutory requests received from relevant public authorities/agencies;
- for any purpose required by law or regulation;
- for disciplinary purposes arising from your conduct or your ability to perform your job requirements;
- with other employee data, to enable the Company to make decisions and/or policies concerning its employees generally;
- with other employee data, to assist in the Company's business and financial monitoring, planning and decision making;
- to enable external and internal auditors to conduct regular reviews of people management within the Company;
- to support any business, administrative or security function required by the Company's operations, including, but not limited to: communication and processing systems; accident/sickness insurance; security of staff, systems and premises (CCTV; card entry systems; IT security systems); telephone recording; contingency planning; systems development and testing; monitoring internet and telephone usage;
- to support the Company's marketing and business development activities and
- to contact relevant people in the event of emergencies.

The Company may disclose your details to verify or obtain additional information about you from third parties including education institutions, present and past employers.

For the purposes stated above, where relevant your personal information will be disclosed to managers and authorised staff within the Company including the HR department, your line manager and their delegates. Other than those listed below, your details will not be revealed to any external body, unless the Company has your consent or is under a legal obligation or entitlement or other duty to do so. When your details are disclosed to an external body, no more details will be given bout you than are necessary. The external bodies to which we may disclose your personal information are:

- any agent, contractor or third party service supplier providing administrative, payroll, telecommunications, computer, general insurance, accident and medical insurance, pension, legal or other services to the Company in connection with its business operations;
- any other person under a duty of confidentiality to the Company including, but not limited to, our external auditors;
- any business contact of the Company where it is necessary for the operation of the Company's business that such persons are given the contact or other details of an employee of the Company;
- any lawyer or firm of solicitors in connection with legal proceedings, to obtain legal advice, or whenever necessary to support the Company's legal rights;
- in the case of the merger or acquisition of all or any part of the Company's business, any actual or proposed purchaser, merger partner or their legal and financial representatives.

Unless special circumstances your personal information will be retained following your departure from the Company, or as otherwise determined by applicable law. In the event that you wish data relating to you to be destroyed following your departure from apetito please contact the HR director. Please bear in mind that not all data can be destroyed as some of it must be preserved under statutory requirements.

Appendix 2

DATA PROTECTION AND PRIVACY STATEMENT – JOB APPLICATIONS

apetito Limited ("the Company") respects the privacy of the personal information provided by you, or by any other person, in connection with your application for employment. This Statement explains how your information will be used and protected.

Your personal information will be used to determine your suitability for a position within the Company and, if applicable, your terms of employment or engagement. Your details may also be included in management information, which the Company uses to monitor its recruitment initiatives and equal opportunities policies. The Company recognises that some information held in the equal opportunities policy will be sensitive personal data and will not be disclosed without your explicit consent. Your details may be held manually or electronically (such as on the Company's databases available to authorised users).

The Company may disclose your details to verify or obtain additional information about you from third parties including education institutions, present and past employers and, if applicable, credit reference agencies. (Credit reference agencies keep details of searches. You can contact us to find out which agencies have been used, if any.)

For the purposes stated above, your details will be disclosed to managers and authorised staff within the Company.

Other than those listed below, your details will not be disclosed to any external body unless you have consented or the Company is under a legal obligation or entitlement or other duty to do so:

- Agents, contractors or third party service suppliers providing services to support the Company's business operations;
- Persons under a duty of confidentiality to the Company including auditors and lawyers;
- Any lawyer or firm of solicitors in connection with legal proceedings, to obtain legal advice or whenever necessary to support the Company's legal rights;

- Any person to whom we may transfer our rights and obligations under any agreement we may have with you.

If your application is unsuccessful, your details will be retained by the Company as part of its poll of potential candidates. Should you not wish apetito to retain your details please let us know.

Where can I get further advice?

Further advice is available from the HR team or your HR representative.

This policy is intended to be used for guidance only and does not rise to any contractual entitlement on the part of the employees. *apetito* reserves the right to review and amend, or withdraw this policy at any time.
