Data Protection and processing Policy

Introduction

Apple A Day Supply is required to gather and use certain information about individuals. This can include employees, schools and other people that Apple A Day Supply 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.

Data Protection Law

The General Data Protection Regulations (GDPR 2018) describes how organisations must collect, handle and store personal information. These rules apply whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The General Data Protection Regulations is underpinned by six important principles. These determine that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Be secure and in a system that permits the easy identification of the data subject

Data Protection Risks

This policy helps to protect Apple A Day Supply from some very real data security risks, including:

• Breaches of confidentiality. For instance, information being given out inappropriately or sending information to the wrong person

• Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them

Apple A Day Supply,
21 A Paxcroft Farm, Trowbridge, Wilts,
BA14 6JB
01225 302011
info@appleadaysupply.co.uk
www.appleadaysupply.co.uk

• Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data, laptops were stolen, or documents weren't stored safely

Data Protection Responsibilities

All Apple Day employees are responsible for ensuring that company data is handled correctly. Apple A Day Supply have an allocated lead for Data Protection called the Data Controller. The person responsible for this is Gemma Hector but it is also the responsibility of Office Management to oversee.

This person's role is to:

- Keep up with current legislation and ensure changes are made within company policies when and where necessary
- Regularly assess company procedures for collecting, storing and disposing of data
- Ensure that all new staff are trained within data protection and that all members of staff receive training yearly
- Decide upon record management procedures
- Ensure that contracts with third parties are following data protection policy and that a signed contract is obtained
- Oversee the monitoring and reporting of records
- Assess risks associated with collecting, storing and sharing data
- Ensure all computers are well maintained and regularly updated with appropriate software to prevent a cyber attack
- Ensure the companies registration with Information Commissioners Office is kept up to date
- Report any breaches of data to the Information Commissioners Office within 72 hours

Everyone who works for or with Apple A Day has responsibility for ensuring data is collected and stored correctly. To ensure that this is done in line with data protection principles, Apple A Day staff must ensure:

- That we obtain permission from employees about data collected
- That we inform them of what information is kept and how it is stored

- That paper documents are kept in lockable boxes/drawers in the office, in a lockable building
- Office staff use lockable memory sticks and that data is kept on this
- Ensure that data is not kept longer than necessary (six years from employee leave date)
- That employee bank details are destroyed following receipt of their Leavers Form
- That the people that are accessing data only require it for their work
- Ensure that data is not disclosed to unauthorised people, either within the company or externally
- That data is reviewed often and updated in the form of yearly reviews, or reviews of paperwork if there is a gap of longer than three months employment
- That data printouts are shredded and disposed of securely when no longer required
- That data that is passed on is done so legitimately and solely for the purposes of work. Any other data, such as application forms, will only be passed on if we have the individual's permission
- That data files are regularly backed up
- That strong passwords are used and that they are never shared
- Employees request help from their manager, or the Data Protection Officer, if they are unsure about any aspect of data protection, or if there has been any breach of policy

Data Collected

This applies to all data that the company holds relating to identifiable individuals, including:

- Name, address and contact information
- Identification such as passport, driver's license for DBS checks
- Bank details
- Photos
- Certificates e.g. Postgraduate degree (PGCE), Undergraduate (if subject specific)
- Safeguarding and Prevent, First Aid, and anything else deemed necessary by our staff
- References
- Notes on any feedback received, disciplinary etc.

All the above documents are in paper files in the form of application forms, interview notes, references, copies of ID, copies of certificates and the sign-up paperwork (contract, bank details, Disqualification of Association and Health Questionnaire).

We also store this electronically across lockable memory sticks, back up hard drive, and on our CRM system. This includes any notes on feedback, CPD courses attended and any issues/concerns that are added to their personal profiles.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the manager or Data Protection Lead.

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:

- When not required, the paper or files should be kept in a locked box, drawer or filing cabinet
- Employees should ensure that paper and printouts are not left where unauthorised people could see them, for example 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 (such as a hard drive), these should be kept locked away securely when not being used
- Data should only be stored on lockable memory sticks. Data should never be saved directly to laptops or other mobile devices, such as tablets or smart phones. If, for any reason, any data needs to be saved on laptops, this should be deleted immediately after use
- Data should be backed up frequently
- All servers and computers containing data should be protected by approved security software and a firewall
- Data kept on our CRM system should be kept secure through responsible and secure password management
- Data should not be kept on personal smart phones or personal laptops

Data Use and Outsourcing

Personal data is of no value to Apple A Day Supply unless the business can make use of it. We only collect and share data deemed necessary for the role. Below are the reasons why we collect and share data.

In office:

• For Safeguarding reasons, to complete DBS checks, Secure Access Checks and ensure that employees are suitable to work with children

• To ensure that staff have the relevant qualifications

For third parties:

• Teacher profiles are shared with schools that have data on them such as name, DOB, TRN, DBS information, certification and qualifications. This is to ensure that schools can follow their own safeguarding practices

• Apple A Day use Gooding Accounts for payroll account management. Personal data such as name, DOB, NI number and bank details are passed on to them to enable them to pay members of staff

All third parties are subject to sign a contract provided by Apple A Day which clearly identifies their obligations to follow Apple A Day's data protection procedures

Any information shared that is deemed out of the norm will be recorded in the decision log, with details of who requested, dates, reasons and the decision reached

Disclosing Data for Other Reasons

In certain circumstances, the General Data Protection Regulations allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.
Under these circumstances, Apple A Day Supply will disclose requested data. However, the Data Lead will ensure the request is legitimate, seeking assistance where necessary.

Data Disposal Procedures

Apple A Day only keep records that are necessary to the needs of the company. We have therefore decided on a six year limit for holding data on

employees. Therefore, six years from leaving, all paperwork must be disposed of appropriately, ensuring it is shredded. It is the responsibility of all members of staff to ensure that this is done and approved by the Data Protection Lead.

Spreadsheets that contain employee start and end dates must be checked regularly to ensure that staff know when files need to be destroyed. Any electronic files must be deleted from our CRM system, memory sticks and the back-up hard drive.

If there are any files for people who applied but didn't work for us, these will also be destroyed after three months. Office staff must routinely check files to ensure that this is done within the time frame specified.

Individuals may have their files destroyed before this date upon request, and subject to the knowledge of the Data Protection Lead.

Incident Management

An information security incident is any event that has the potential to affect the confidentiality, integrity or availability of company information in any format. Examples of information security incidents can include, but are not limited to:

• The disclosure of confidential information to unauthorised individuals

• Loss or theft of paper records, data or equipment such as tablets, laptops and smartphones on which data is stored

• The transfer of data or information to those who are not entitled to receive that information

• Attempts to gain unauthorised access to computer systems, e, g hacking

• Virus or other security attack on IT equipment systems or networks

• Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information left unlocked in accessible areas

• IT equipment left unattended when logged-in, without locking to stop others accessing information

It is imperative that actual or suspected security incidents are contained as quickly as possible to manage and minimise the potential impact to the company and individual. Staff and third parties i.e. schools must report all events, threats and weaknesses to management and Data Lead Officer so that incidents can be assessed, contained and resolved or prevented. Any data security incidents must then be reported to the necessary bodies (such as ICO) within 72 hours.

Any employee or third party found to have breached this policy may be subject to Apple A Day disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s). If any employee, contracted third party or agent of Apple A Day Supply does not understand the implications of this policy or how it applies to them they should seek advice from the Data Lead Officer, Gemma Hector.

Privacy Notice and Access Request

All individuals who are the subject of personal data held by Apple A Day Supply are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

Should an individual contact the company requesting this information, this is called a subject access request (SAR). Subject access requests from individuals should be made by email, addressed to the Data Control Lead at ghector@appleadaysupply.co.uk.

The Data Control Lead will aim to provide the relevant data within 14 days.

The Data Control Lead will always verify the identity of anyone making a subject access request before handing over any information.

All requests will be documented within the decision log.

Social Media

This policy provides guidance for employee use of social media in relation to Apple A Day Supply. This includes blogs, social networking sites, online forums, chat

rooms and any other site that permits users to share information with others.

The following principles apply to professional use of social media on behalf of Apple A Day Supply, as well as personal use of social media when referencing Apple A Day Supply.

• Employees must know and adhere to the Employee Handbook and Company Code of Conduct in reference to Apple A Day Supply when using social media

• Employees should not post any information about Apple A Day to their personal accounts, unless sharing the original post made by Apple A Day. The Employee should seek approval before posting any images or information to their personal profile

• Employees must be aware of the consequences of sharing images or information about Apple A Day Supply. This includes the length of time that this information is public, and also the reputation of the Employee and the Company

• Employees must be aware that Apple A Day may observe any content or information that they make available on social media. Employees must use their best judgment in posting material that is neither inappropriate nor harmful to Apple A Day, its customers and its employees

• Examples of prohibited content include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous or that can create a hostile working environment

• Employees should not post or publish any data that is deemed confidential. This includes profiles of schools, teachers and any other employee, partner or colleague. If there are questions about what is deemed as confidential data, employees should check with a Manager

• If press and media attention is generated following activity on social media networks or other sites, employees should refer any enquiry to a Manager

• If employees encounter a situation while using social media that threatens to become antagonistic, they should disengage from any communication in a polite manner, and refer it to a Manager

• Employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property. This includes using logos of our partnership companies, i.e. APSCo

• Use of personal social media networks is not permitted during working hours, unless on a break. During work hours, company laptops are to be used for business purposes only, including social networking sites linked to Apple A Day i.e. Facebook, LinkedIn, Twitter

• It is highly recommended that employees keep Apple A Day related social media accounts separate from personal accounts wherever possible. Currently, this is only an issue with Facebook and LinkedIn

• When no longer employed by Apple A Day, individuals must remove Apple A Day as their current job from their personal social media

Emails

This policy involves the use of personal email accounts and work email accounts. Employees should adhere to the following guidelines when emailing anything that is business related to Apple A Day.

• It is not permitted for any employee to use their personal email account to share any content or information about Apple A Day. Any email containing data, information or content related to Apple A Day, its employees, clients or partnership companies must be sent using your Apple A Day email account

• Personal email accounts should not be given to any prospective or existing employee, client or partnership company as a point of contact for business related information. This includes having your personal email as a point of contact on your LinkedIn profile

• An employee's Apple A Day email account must only be used for business-related matters. Any email sent from your work account must be business related, and not personal

• Personal email accounts may only be accessed from an employee's work laptop during breaks

• Employees should not send emails containing any personal data from their work accounts to their personal accounts or vice versa. This prevents any data relating to Apple A Day becoming unsecure

• No-one should have access to an employee's login details, unless authorised by a Manager. All passwords must be kept in a secure place

• Work emails should not be accessed from any device other than your work laptop

Home and Mobile Working

Homeworking refers to any work relating to Apple A Day Supply that is not carried out in the office. Homeworking is not permitted unless authorised by a Manager. In the instance that you are required to work at home, it's important to adhere to these guidelines:

• Whilst homeworking is categorised as a type of flexible working, employees should not assume that other aspects of flexible working (such as amended hours) are automatically part of a homeworking arrangement. It is expected that employees are working their normal hours as instructed by a Manager

• Employees should also always be available as a point of contact during these hours. They should keep their phones on them at all times, unless on a break

• Employees should not leave their place of working unless they have their appropriate equipment with them i.e. phone and laptop, or if the employee is on a break. Employees must notify a colleague or Manager when they are taking their breaks and when they are unavailable as a point of contact

Below is guidance for employee use of work laptops and anything linked to Apple A Day that is transported outside of the office:

• Laptops should not be taken home under any circumstances, unless authorised and deemed necessary by a Manager

• If laptops are taken home, it's important for employees to ensure that no-one has the password to their lockable memory stick

Laptops must be locked in the car boot during transport

• Any data that is saved onto a lockable memory stick must remain there and not be transferred onto personal memory sticks, laptops or other storing devices, including the work laptops

- Laptops and lockable memory sticks must be stored safely and securely when not in use

- When working with confidential data, it's important that nobody outside of the office has access or the ability to view it. Any work involving confidential data should be carried out in the office, unless authorised by a Manager. This includes teacher profiles, school profiles or any other data linking to employees, colleagues or partnership companies
- If date/confidential information is taken out of the office, it must be done so in a lockable briefcase
- Personal phones should not be used for business related use. This includes work emails, social networking sites (see Social Media policy for list) and our CRM system, unless authorised by a Manager

Apple A Day staff agree to follow the above procedures

Enforced: September 2013

Reviewed: March 2014, 2015,2016,2017 and 2018

Apple A Day Supply,
21 A Paxcroft Farm, Trowbridge, Wilts,
BA14 6JB
01225 302011
info@appleadaysupply.co.uk
www.appleadaysupply.co.uk

Type of Data	Risk	Measures in Place
Files, contracts, ID	Office is burgled Key accessed Data viewed by others	Key Hidden Office locked Alarm in office Ensure data is locked away
CRM system – school, teacher contact info, feedback	Computer hacked Computer accessed	Secure software & passwords Lock screen when away from desk
Data on memory sticks e.g: teacher profiles	Stick stolen Stick accessed by others	Only access data from work computers Do not share log-ins Memory stick password protected Don't share passwords