Cotteswold Dairy

Data Protection Policy

Context & Overview

Key Details:

- Policy prepared by: Mark Crosby, ICT Business Analyst
- Last updated: Monday, 15/05/2017
- Version: 1.1
- Approved by board / management on: Friday, 12/05/2017 (TW)
- Policy became operational on: 12/05/2017
- Next review date: xx/xx/xx

Introduction:

Cotteswold Dairy Ltd and all group undertakings ("the company") gathers and uses certain information about individuals, businesses as part of its day to day business. These include customers, suppliers, business contacts, employees 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 policy exists:

This data protection policy ensures Cotteswold Dairy Ltd;

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers, suppliers and other stakeholders
- 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 on other materials. 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, 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 data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, Risks & Responsibilities

Policy Scope:

This policy applies to:

- The head office of Cotteswold Dairy Ltd
- All depots of Cotteswold Dairy Ltd
- All employees of Cotteswold Dairy Ltd
- All contractors, suppliers and other people working on behalf of Cotteswold Dairy Ltd

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, but is not limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Bank account and credit card details

Data Protection Risks:

This policy helps to protect Cotteswold Dairy Ltd from some data security risks, including:

- Breaches of confidentiality – *i.e. Information being given out inappropriately*
- Failing to offer choice – *i.e. All individuals should be free to choose how the company uses data relating to them*
- Reputational damage – *i.e. The company could suffer if hackers successfully gained access to sensitive data*

Responsibilities:

Everyone who works for or with Cotteswold Dairy Ltd 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, the following people have key areas of responsibility:

- The board of directors are ultimately responsible for ensuring that Cotteswold Dairy meets its legal obligations
- The Data Protection Officer(s), Tom Wood / Mark Crosby is responsible for:
    - ✓ Keeping the board 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 Cotteswold Dairy Ltd holds about them (also called 'subject access requests')
    - ✓ Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
- The IT Officer, [Mark Crosby] is 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 used to store or process data. For instance, cloud computing services
- The Marketing Manager, [Roseanne McEwan] is responsible for:
    - ✓ Approving any data protection statements attached to communications such as emails and letters

- ✓ Addressing any data protection queries from journalist or media outlets like newspapers
- ✓ Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their role**
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line manger
- Cotteswold Dairy Ltd **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
- Employees should request help from their line manager or the Data Protection Officer 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 the IT Officer, [Mark Crosby] or Data Protection Officer(s). When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see or access it.

These guidelines also apply to data that is usually stored electronically but has been printed out for any reason:

- When not required, the paper file should be **kept in a locked drawer or filling cabinet**
- Employees should make sure paper and printouts **are not left where unauthorised people could see them**
- **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** (like a CD or DVD), 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 approved **cloud computing services**
- Servers containing personal data should be **sited in a secure location**, away from general office space
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures
- Data should **never be saved locally** to laptops or other mobile devices like tablets or smartphones
- All servers and computers containing data should be protected by **approved security software and a firewall**

Data Use

It is when personal data is accessed 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 and laptops are always locked** when left unattended
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure
- Data must be **encrypted before being transferred electronically**. The IT Officer, [Mark Crosby], can explain how to send data to authorised external contacts
- Personal data should **never be transferred outside of the European Economic Area**
- 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 Cotteswold Dairy Ltd to take reasonable steps to ensure data is kept accurate and up to date.

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.** For instance, by confirming a customer's details when they call
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number or email address, it should be removed from the database
- It is the Marketing Manager, [Roseanne McEwan] 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 Cotteswold Dairy Ltd 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**

In 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 Data Protection Officer(s) [Tom Wood and Mark Crosby. The Data Protection Officer(s) can supply a standard request form, although individuals do not have to use this. Individuals will be charged £10 per subject access request. The Data Protection Officer(s), will aim to provide the relevant data within 14 days. The Data Protection Officer(s) will always verify the identity of anyone making a 'subject access request'

Disclosing Data for 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, Cotteswold Dairy Ltd will disclose requested data. However, the Data Protection Officer(s), will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary

Providing Information

Cotteswold Dairy Ltd 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 [This is available on request. A version of this statement is also available on the company's website.]