PRIVACY & DATA SECURITY POLICY

What is this policy for?
The Company is committed to being transparent about how it collects and uses the personal data of its workforce, suppliers, customers and during any recruitment process and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

We are pleased to confirm that Suncream Dairies fully adheres to the Ethical Trading Initiative (ETI) Base Code. The ETI Base Code reflects key international standards and is founded on the conventions of the International Labour Organization (ILO). Our commitment to these principles underscores our dedication to ethical business practices and responsible sourcing.

Who is this policy for?
This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. This policy also applies to the personal data of clients and suppliers, or other personal data processed for business purposes.
Definitions
"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
"GDPR protected data" is any confidential information relating to an individual, supplier or customer. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.
Data protection principles
The Company processes GDPR protected data in accordance with the following data protection principles:

- The Company processes personal, customer and supplier data lawfully, fairly and in a transparent manner.
- The Company collects personal, customer and supplier data only for specified, explicit and legitimate purposes.
- The Company processes personal, customer and supplier data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Company keeps accurate personal, customer and supplier data and takes all reasonable steps to ensure that inaccurate data is rectified or deleted without delay.
- The Company keeps GDPR protected data only for the period necessary for processing.
- The Company adopts appropriate measures to make sure that GDPR data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Where the Company processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

The Company will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

PRIVACY & DATA SECURITY POLICY

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file in hard copy or electronic format, or both. The periods for which the Company holds HR-related personal data are contained in its privacy notices to individuals.

The Company keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights
As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests
Individuals have the right to make a subject access request. The Company will provide the individual with a copy of the personal data undergoing processing.

Other rights
Individuals have a number of other rights in relation to their personal data. They can require the Company to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

Data security
The Company takes the security of GDPR protected data seriously. The Company has internal policies and controls in place to protect such data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the Company engages third parties to process GDPR data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Individual responsibilities

- Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let the Company know if data provided to the Company changes, for example if an individual changes address or changes his/her bank details.
- Individuals may have access to the personal data of other individuals and of our customers and suppliers in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the Company relies on individuals to help meet its data protection obligations to staff and to customers and clients.
- Individuals who have access to GDPR data are required:
    - to access only data that they have authority to access and only for authorised purposes;

- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove GDPR data, or devices containing or that can be used to access GDPR data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store GDPR data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to the Managing Director immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer/supplier data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The Company will provide training to all individuals about their data protection responsibilities as part of the induction process. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.