GDPR DATA BREACH POLICY AND PROCEDURE			
Author:	Human Resources		
Document Reference:	BFHRPO31		
Revision no.	0.3	**Publish Date:**	February 2026
Document status:	Current		
For use by:	All employees of Burgess Farms and its subsidiary Companies.		
Purpose:	To set out clear and consistent guidelines relating to any breach, or suspected breach, of personal data in line with data protection legislation, including General Data Protection Regulations (GDPR)		
This document supports: *Standards and legislation*	General Data Protection Regulation (GDPR) 2018 Data Protection Act (DPA) 1998		
Key related documents:	Data Protection Policy Employee Handbook Disciplinary Policy and Procedure Grievance Policy and Procedure Equal Opportunities Policy & Procedure Recruitment Policy & Procedure CCTV Policy Health & Safety Policies Whistleblowing Policy		
Review date:	Changes to legislation / Changes to Company policy		

do the RIGHT thing, in the RIGHT way

OWN it, be PROUD of it

find new SOLUTIONS, shape our FUTURE

work TOGETHER, win TOGETHER

POSITIVE CUSTOMER experience, every time

Contents

Definitions

"Company" means Burgess Farms Ltd

"Subsidiary Companies" means all Companies owned by Burgess Farms Ltd.

1. Policy Statement

The Company is committed to ensuring the security of personal data in our possession.

The General Data Protection Regulations (GDPR) requires that we must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. This policy sets out how we deal with a data security breach.

The Company reserves the right to amend the policy and procedure as necessary to meet any changing legislation or business requirements. This policy does not confer any contractual rights on employees. The Company's policy is designed to ensure transparency regarding the processing of personal data. Processing includes (but is not limited to) collecting, recording, storing, amending, reviewing, using and deleting personal data.

2. Key Principles

In the course of your work with our Company you are likely to collect, use, transfer or store personal information about employees, clients, customers and suppliers, for example their names and home addresses. The UK's data protection legislation, including the General Data Protection Regulations (GDPR) contains strict principles and legal conditions which must be followed before and during any processing of any personal information.

The aim of this policy is to enable the Company to deal swiftly with any data breaches, or suspected data breaches, ensure GDPR guidelines are followed and that corrective measures are put into place to avoid similar occurrences.

This policy does not form part of a contract of employment. However, it is mandatory that all employees, workers or contractors must read, understand and comply with the content of this policy and must attend identified associated training relating to its content and operation as indicated within your job role. Failure to adhere to this policy is likely to be regarded as a serious disciplinary matter and will be dealt with under the Company's Disciplinary Policy and Procedure.

3. Scope

This policy applies to all employees employed by Burgess Farms (Produce World Group) and its subsidiary companies. This policy is non-contractual and may be varied or revoked by the Company at any time with or without notice. It also applies to any worker, contractors, work-experience, apprentices, agency staff or any other person working on or visiting the Company premises or working for the Company in any capacity.

4. Responsibilities

All employees, workers, contractors, work-experience, apprentices, agency staff or any other person working on or visiting the Company premises or working for the Company in any capacity, are responsible to personal data security and ensuring that any breach, or suspected breach, is reported to the business.

5. What is a Personal Data Breach?

The Information Commissioner's Office (ICO) states that a personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

6. Action to be taken in the event of a Data Breach

6.1 Containment and Recovery:

The immediate priorities are to:

- contain the breach;
- assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- to limit the scope.

In the event of a security incident or breach, staff must immediately inform the Data Protection Champion.

The Data Protection Champion will take the lead on investigating the breach. In the event where the Data Protection Champion is absent for whatever reason, the Group Risk Manager or Head of HR will take the lead on investigating a breach.

Steps to take where personal data has been sent to someone not authorised to see it:

- inform the recipient not to pass it on or discuss it with anyone else;
- inform the recipient to destroy or delete the personal data they have received and get them to confirm in writing that they have done so;
- explain to the recipient the implications if they further disclose the data; and
- where relevant, inform the data subjects whose personal data is involved what has happened so that they can take any necessary action to protect themselves.

6.2 Assessing the Risk:

Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

Examples of the type of questions to consider:

What type of data is involved?	
How sensitive is it?	
If data has been lost or stolen, are there any protections in place such as encryption?	
What has happened to the data?	i.e. If stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk
How many individuals' personal data are affected by the breach?	
Who are the individuals whose data has been breached?	Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
What harm can come to those individuals?	Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?	
Is anything you can do to recover any losses and limit the damage the breach can cause?	

6.3 Notifying the ICO and Individuals

a) Who is responsible?

In our business, the Data Protection Champion is the point of contact for staff and the ICO on this policy and on all matters relating to data protection.

The Data Protection Champion is also responsible for notifying the ICO and individuals (where applicable) of relevant personal data breaches.

b) What breaches do we need to notify the ICO about?

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, we must notify the ICO; if it's unlikely then we don't have to report it.

If we decide we don't need to report the breach, we need to be able to justify this decision, and we should document it.

c) When to notify the ICO and dealing with delays

Notifiable breaches must be reported to the ICO without undue delay, but not later than 72 hours after becoming aware of it.

If we don't comply with this requirement, we must be able to give reasons for the delay.

In some instances, it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Where that applies, we should provide the required information in phases, as long as this is done without undue further delay.

d) Breach information to the ICO

When reporting a breach, we will provide the following information:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned;
  - and the categories and approximate number of personal data records concerned;
- our contact person i.e. Data Protection Champion;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

e) Individuals

Where notification to individuals may also be required, the Data Protection Champion will assess the severity of the potential impact on individuals as a result of a breach and the likelihood of this occurring. Where there is a high risk, we will inform those affected as soon as possible, especially if there is a need to mitigate an immediate risk of damage to them.

g) Information to individuals

The Data Protection Champion will consider who to notify, what we are going to tell them and how we are going to communicate the message. This will depend to a large extent on the nature of the breach but will include the name and contact details of our Data Protection Champion (where relevant) or other contact point where more information can be obtained; a description of the likely consequences of the personal data breach; and a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

The breach need not be reported to individuals if:

- We have implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach;
- We have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- It would involve disproportionate effort (in this case a public communication may be more appropriate).

In the case of a breach affecting individuals in different EU countries, we are aware that the ICO may not be the lead supervisory authority. Where this applies, the Data Protection Champion, should establish which European data protection agency would be the lead supervisory authority for the processing activities that have been subject to the breach.

h) Third parties

In certain instances, the Data Protection Champion may need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals.

i) Document all decisions

The Data Protection Champion must document all decisions that we take in relation to security incidents and data breaches, regardless of whether or not they need to be reported to the ICO.

6.4 Evaluation and Mitigation Steps

The Company will investigate the cause of any breach, decide on remedial action and consider how we can mitigate it. As part of that process we will also evaluate the effectiveness of our response to incidents or breaches. To assist in this evaluation, we will consider:

• What personal data is held, where, and how it is stored
• Risks that arise when sharing with or disclosing to others • This includes checking the method of transmission to make sure it's secure and that we only share or disclose the minimum amount of data necessary
• Weak points in our existing security measures such as the use of portable storage devices or access to public networks
• Whether or not the breach was a result of human error or a systemic issue and determine how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps
• Staff awareness of security issues and look to fill any gaps through training or advice
• The need for a Business Continuity Plan for dealing with serious incidents
• The group of people responsible for reacting to reported breaches of security

7. Review

This document will reviewed by us in line with any changes to legislation or changes to Company policy.

8. Complaints

Where a subject of personal data is not satisfied with how we have handled a data breach, we must manage this as a complaint.

We must advise the subject that if they remain unhappy with the outcome they may complain to the Information Commissioners Office (ICO) or take legal action against us.

9. Breach of Policy

Firstly, a serious breach of data protection is likely to be a disciplinary offence and will be dealt with under the Company's disciplinary procedure.

Additionally, if you knowingly or recklessly dispose of personal data in breach of this policy and data protection legislation, including the GDPR, or fail to report a data breach (or suspected data breach), you may be held personally criminally accountable for any such breach or failure.

All employees must co-operate fully in any investigation into suspected breaches of this policy.

10. Document Control

Revision	Action	Author	Date
0.0		NMT	07.02.2020
0.1	Contents Page Amended	RMI	10.02.2020
0.2	Company Logo Update	RC	22.08.2022
0.3	Formatting and updated values	GT	27.02.2026