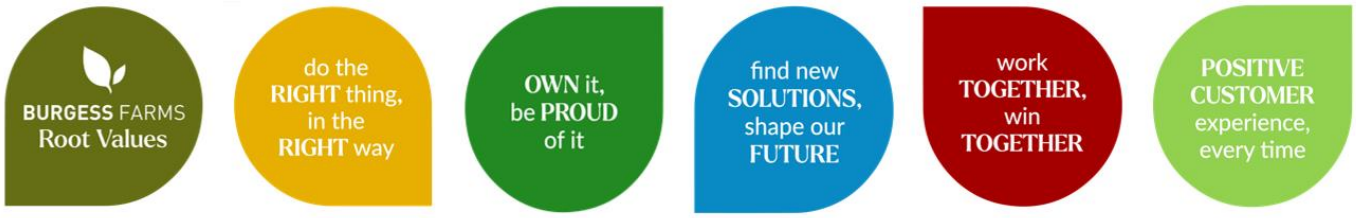
BURGESS FARMS

GDPR DATA SUBJECT ACCESS REQUEST POLICY AND PROCEDURE			
Author:	Human Resources		
Document Reference:	BFHRPO33		
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 subject access request relating to 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		



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 subject access requests relating to personal data seriously and follow strict guidelines on how these should be dealt with. This policy sets out how we deal with a subject access request.

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.

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.

To deal swiftly with any subject access requests, ensuring GDPR guidelines and timeframes are adequately followed and that steps are taken to ensure that the request is valid.

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 for ensuring data security and that any subject access request is passed on to the appropriate person in line with the guidelines contained within this policy.

5. Procedure

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Our business must comply with the requirements of the General Data Protection Regulations (GDPR) and we must be able to demonstrate compliance to the Information Commissioner's Office (ICO).

Upon receipt of a request for information our internal policy is as follows:

5.1 Handling a Request

The Data Protection Champion is responsible for the handling of Subject Access Requests (SAR) in our business. If the Data Protection Champion is not available for a period of more than 2 days, the responsibility will lie with the Group Risk Manager or Head of HR.

The duties of the Data Protection Champion include but are not limited to:

- Log the receipt and fulfilment of all requests received from a data subject/the person making the request/ requestor to see his or her personal information
- Acknowledge the subject access request (SAR)
- Verify the identity of any person making a SAR
- Maintain a database on the volume of requests and compliance against the statutory timescale
- Verify whether we are the controller of the data subject's personal data
- Check if we are not a controller, but rather a processor. If so, inform the data subject and refer them to the actual controller. This needs to be recorded in writing
- Where applicable, decide if a request is excessive, unfounded or repetitive and communicate this to the requestor
- Decide if an exemption applies
- If a SAR is submitted in electronic form, any information should preferably be provided by electronic means as well

5.2 Oral or Written Requests

SAR's can be made in writing, electronically, or verbally.

If a member of staff is in any doubt if a certain situation has given rise to a SAR, contact the Data Protection Champion by email providing full details of the incident. Staff should do this without delay and certainly within two business days.

Where a member of staff receives a subject access request, they must email the relevant information to the Data Protection Champion without delay and certainly within two business days.

5.3 Verifying the Requestor's Identity

The requestor must supply valid evidence to prove their identity.

We may verify the requestor's identity either through a phone call where we ask questions that only the requestor will know the answers to or by requesting forms of identification.

We accept the following forms of identification:

- Current UK/EEA Passport
- UK Driving Licence
- Financial Statement issued by bank, building society or credit card company
- Utility bill for supply of gas, electric, water or telephone landline

5.4 Processing the Request

The Company's aim is to determine what information the requestor is asking for. If the request is not clear, or where if we process a large quantity of information about an individual, the GDPR permits us to ask the individual to specify the information the request relates to. Where this applies, we will proceed with a request for additional information.

We must verify whether we process the data requested. If we do not process any such data, we must inform the data subject accordingly.

We must respond to the data subject within 30 days of receiving the request as valid. This is a requirement under the GDPR.

Any employee, who receives a request from the Data Protection Champion to locate and supply information relating to a SAR, must make a full exhaustive search of the records which they are responsible for or owns. This may include but is not limited to emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks), recordings, paper records in relevant filing systems.

The Data Protection Champion should check whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the requestor; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

All the information that has been requested must be provided unless an exemption can be applied (see below). Information must be supplied in an intelligible form and we will explain acronyms, codes or complex terms.

5.5 No Charge for the Request (with exceptions)

The Company will provide a copy of the information free of charge, as per the GDPR rules. However, we may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The Company will also charge a reasonable fee to comply with requests for further copies of the same information. We understand that this does not mean that we can charge for all subsequent access requests.

Where applicable, the Data Protection Champion will determine the 'reasonable fee' that must be based on our administrative cost of providing the information.

5.6 Excessive, Manifestly Unfounded or Repetitive Requests

The Company will provide a copy of the information free of charge, as per the GDPR rules. However, we may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The Company will also charge a reasonable fee to comply with requests for further copies of the same information. We understand that this does not mean that we can charge for all subsequent access requests.

Where applicable, the Data Protection Champion will determine the 'reasonable fee' that must be based on our administrative cost of providing the information.

5.7 Complex Requests

As stated, the Company has to respond to a SAR within 30 days. If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within 30 days.

Where it is decided not to act on the request of the data subject, we need to inform the data subject of this decision without delay and at the latest within 30 days of receipt of the request.

5.8 Response to the Requestor

After processing the SAR, the Company's response to the requestor will include:

- the purpose(s) of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third party countries or international organisations, including any appropriate safeguards for transfer of data;
- the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with the ICO;
- if the data has not been collected from the data subject: the source of such data;
- the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the requestor.

5.9 Exemptions

If a member of staff believes that we have a valid business reason for an exemption, please inform the Data Protection Champion without delay by email.

Exempt information must be redacted from the released documents with an explanation of why that information is being withheld.

6. Review

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

7. 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.

8. 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.

9. 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	16.08.2022
0.3	Formatting and updated values	GT	27.02.2026