Carrs Billington Agriculture Pension Scheme ("the Scheme")

Data protection policy

This policy is adopted by the Trustee board, or any individual Trustee (each "a Trustee" and together "the Trustee") of the Scheme. In the course of managing the Scheme, the Trustee and their service providers collect and process information about members of the Scheme and their beneficiaries. The Trustee is legally responsible for ensuring that this information ("Personal Data") is processed in accordance with the law and with individuals' rights in respect of their Personal Data.

This policy sets out how the Trustee approach to compliance with the key rules governing the use of such Personal Data.

1) Data Controllers, Data Processors, Data Subjects, and processing activities

The Trustee of the Scheme, the Scheme Actuary, the Scheme legal adviser, and the sponsoring employer are joint "Data Controllers". The Scheme's Administrator and other third parties who process Personal Data on behalf of the Trustee are referred to as "Data Processors".

The Scheme Actuary will be appointed by the Trustee and will be employed by an Actuarial Consultancy, detailed through a contract of services.

However, the Data Controllers can delegate certain duties to the following Data Processors that have access to Scheme members' and beneficiaries' Personal Data:

Role	**Access to data**
Administrator (including the Sponsoring Employer in respect of pensioner payroll)	Manages Scheme members' Personal Data so the correct benefits can be paid to the correct members and beneficiaries. Maintains addresses and other contact details so that benefit statements and newsletters may be issued.
Secretary to the Trustee	Personal Data relating to specific member queries, managing specific Scheme or governance projects.
Actuarial consultant	Personal Data required to undertake valuations, set actuarial factors, set the transfer basis, relating to specific member queries, managing specific projects.
Fiduciary manager	Personal Data required for cashflow analysis and investment strategy reviews (but rare for data used to be personal data).
Auditor	Personal Data relating to specific member events in the accounting year.
Legal adviser	Personal Data relating to specific member queries and specific projects.
AVC provider(s)	Personal Data for members with AVCs.

Role	Access to data
Annuity provider	Manages database and files of all annuitants' Personal Data so they can pay the agreed benefits to the relevant members and beneficiaries.

The Trustee has contracts in place with all of their Data Processors that include terms requiring the data processor to process data in accordance with the United Kingdom General Data Protection Regulation (UK GDPR), including processing data only for the purpose for which it has been collected, limiting the storage of data for no longer than required, and ensuring the security of the data processed.

A Data Processor may delegate certain tasks to sub-processors if permitted in the terms of their appointment. The Data Processer has the contractual relationship with the sub-processor so is liable for any data protection breaches by the sub-processor. Where a Data Processor delegates certain tasks to a sub-processor, the Data Processor will ensure that a written agreement is put in place setting out the terms on which that sub-processing takes place.

All Scheme members, beneficiaries and potential beneficiaries are the "Data Subjects". Categories of Personal Data that are processed are all of those required to comply with the Trustee's legal obligations and may include (but are not limited to):

- name
- gender
- address
- date of birth
- National Insurance number
- salary information
- employment history
- marital status
- bank account details: name, date of birth, address etc. for any recipient of any survivor benefits payable from the Scheme

2) Lawful grounds for processing data

The Trustee must have a lawful basis for processing the Personal Data of Scheme members and dependants. The lawful bases under which the Trustee processes Scheme members' and dependants' data are twofold:

- **legitimate interests** – data processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or their Data Processors, i.e. the effective running of the Scheme by the Trustee and Scheme administrator. The Trustee's analysis on this point is set out in section 3 below.
- **compliance with legal obligations** – the Trustee is legally required to pay the correct level of benefits to the Scheme members and their dependants and must process members' and dependants' Personal Data to comply with this legal requirement.

3) Legitimate interests

In relation to legitimate interests, the Trustee's approach is as follows:

(a) Purpose test: is the Trustee pursuing a legitimate interest?

The Trustee's main purpose is to pay members and their beneficiaries the benefits they are entitled to under the rules of the Scheme. It is clearly in members' interests to have the Scheme properly administered and benefits paid when due. So, the Trustee is satisfied that it is pursuing a legitimate interest.

(b) Necessity test: is the processing necessary for that purpose

In this context "necessary" means that the processing must be a targeted and proportionate way of achieving the purpose, as laid out in (a) above. The Trustee cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result. The Trustee is satisfied that administering the Scheme and paying benefits in accordance with the Scheme's rules would not be possible without processing Personal Data.

(c) Balancing test: do the individual's interests override the legitimate interest?

The Trustee has balanced the legitimate interests against the other interests of the members and is satisfied that members' interests are in fact aligned with the Trustee's legitimate interests – members and beneficiaries benefit from the data processing by having the correct benefits paid to them. The Trustee only uses the Personal Data for this purpose, as members would expect, and it is unlikely that processing should result in any detriment to the individuals concerned.

(d) Conclusion

The Trustee is therefore satisfied that following this process it can lawfully process Personal Data based on legitimate interests.

4) Special Category data

Certain sensitive Personal Data is categorised as "Special Category data". This includes data concerning a member's health or sexual orientation, which may need to be processed to administer ill health retirement or pay benefits in the event of a member's death. Provisions in the UK GDPR allow Special Category data to be lawfully processed where:

- the member has given explicit consent to the processing of the Special Category data
- processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Data Controller or the Data Subject in connection with employment, social security, or social protection
- processing is necessary for the establishment, exercise, or defence of legal claims.

When requesting Special Category data to administer ill health or death claims, the Scheme administrators have included appropriate wording on their standard forms to obtain the member's or dependant's consent to process the data provided.

5) Privacy Notice

The Trustee maintains a written record of its processing activities as Data Controller as detailed in the Privacy Notice under Appendix A.

6) Retention of Personal Data

The Trustee has a need to retain Scheme members' Personal Data for their entire lifetime and/or Scheme membership (and those of any beneficiaries in receipt of pension benefits from the Scheme on their death) and beyond. This is required to ensure the correct Scheme benefits are paid and to protect the Trustee against any future claim after a member's death or after they have transferred out of the Scheme.

7) Data Protection Officer

The Trustee has not appointed a Data Protection Officer. The Trustee does not require a Data Protection Officer because they are not:

- a public authority; or
- carrying out large scale monitoring of individuals; or
- carrying out large scale processing of special categories of data or data relating to criminal convictions and offences.

8) Security and access to data

The Scheme administrator manages members' Personal Data held on their behalf by the Scheme. The Trustee has obtained assurances from the Scheme administrator as the Data Processor that it has the appropriate technical and organisational measures in place as required under the UK GDPR to securely process members' data.

The Trustee recognises there is an inherent security risk when transferring data between third parties. In the first instance, data is anonymised or pseudonymised whenever possible but it is recognised there will be instances where this isn't possible for the efficient management of a specific task. When Personal Data is transferred electronically it is either sent via a secure web portal or by encrypted e-mail.

The Trustee may need to use their own devices to access Scheme Personal Data, but do so via encrypted emails website access; any data accessed via members' personal devices is kept to a minimum and should be accessed via a secure platform only and in accordance with the Employer's relevant IT policies.

Vidett as the professional independent trustee, stores a limited amount of members' Personal Data on their secure network systems, as necessary to undertake their role. Employer appointed trustees may store a limited amount of members' Personal Data on their secure work network or in secure paper filing at the workplace.

9) Data breach reporting process

If there has been a Personal Data breach the Trustees must determine whether to make a report to the Information Commissioner's Office (ICO) within 72 hours of the breach occurring. The Trustees will take into account whether the breach posts a high risk to

member's Personal Data, and the likelihood and severity of that breach, when deciding whether to report the breach to the ICO.

If a Personal Data breach is identified by a Data Processor it must be reported to the Trustee, the Secretary to the Trustee or the Scheme Actuary within 24 hours. The Trustee will consider whether the breach must be reported to the ICO and consider taking advice as necessary.

Where a Personal Data breach gives rise to a high risk to an individual's rights and freedoms, the Trustees will notify affected members of the breach without undue delay. All Data Processors have been informed of the Trustee's Data Breach reporting process, which is laid out in the Trustee's Incident Response Plan. The Trustee retains an internal register of all Personal Data breaches whether they need to be reported to the ICO or not.

10) Subject Access Requests

Members have the right to access and receive a copy of their personal data and other supplementary information by making a Subject Access Request ("SAR"). UK GDPR requires the information to be provided within one month of the SAR and the information must be provided free of charge.

The Secretary should be notified within a week of the request being received. The Secretary will liaise with the administrator to acknowledge the request, coordinate the relevant information, and agree the response with the Trustee within one month of the request.

11) Right to be forgotten

UK GDPR gives individuals the right to request that a Data Controller deletes their Personal Data. This is the "right to erasure" also known as the right to be forgotten. The right is not absolute and only applies in certain circumstances. Any right to erasure request must be responded to within one month of receipt.

The right to erasure does not apply if processing is necessary to comply with a legal obligation and there is a legitimate interest in retaining the Personal Data.

There are very limited circumstances under which a request to delete data can be agreed. For example, even if a member has transferred their benefits out of the Scheme, the Trustee will need to retain records of the transfer to challenge any potential future benefit claim.

12) Data transfer within the European Economic Area (EEA)

Following the United Kingdom's withdrawal from the European Union (EU), the EU has formally recognised the UK's high data protection standards and has adopted 'adequacy' decisions allowing data to continue flowing freely between the EEA and the UK.

13) Data transfer outside the European Economic Area (EEA)

The Trustee's policy is not to allow the transfer of data for processing outside the EEA (unless there are suitable and appropriate agreements in place).

Version	Date of Review	Amendments to Policy	Date Adopted by Trustee
2	Feb 2025	VM legal review amendments	18/11/2025

Appendix A – Privacy Notice