The Buccleuch Estates Limited 1974 Retirement Fund

November 2025

General Data Protection, Information Security and Privacy Policy on Fair Processing for The Buccleuch Estates Pension Trustee Company Limited

Claire Petzer – Consultant
Cartwright Benefit Consultants Limited
Marlborough House, Victoria Road South, Chelmsford, Essex CM1 1LN
Telephone: 01245 293300
Email: Claire.petzer@cartwright.co.uk

Contents

Board / Trustee Policy Approval Summary

Policy: General Data Protection, Information Security & Privacy Policy

Policy owner: Risk / Governance Sub-committee

Approved by: Trustee Board

Version	Date policy adopted	Next Review Date	Review frequency	Status
1.0	12.11.2025	November 2026	Annual (or sooner if law / process changes)	Approved

The Buccleuch Estates Limited 1974 Retirement Fund ('Fund')

PART I

1. Introduction and purpose

purpose this document is to formally document the policies the Trustee, The Buccleuch Estates Pension Trustee Company Limited, has adopted in order to meet the requirements the General Data Protection Regulations (GDPR), in relation to Buccleuch Estates Limited 1974 Retirement Fund and together with other documents referenced herein, covers the Trustee obligation to demonstrate accountability in relation to GDPR in respect the Fund. Operational procedures that support this policy are maintained separately in the Trustee Directors' Data Protection Procedures Manual. These procedures may be updated from time to time to reflect changes in practice, legislation, or service provider arrangements, without requiring re-approval of the core policy.

2. Background to GDPR

European General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) was adopted on 27 April 2016 and was designed to enhance privacy laws across Europe and replace all EU member states data protection legislation and also the UK's Data Protection Act 1998 (DPA).

GDPR under the Data Protection Act 2017 took effect from 25 May 2018.

Since 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (regulations concerning marketing and the use websites) and the Data (Use and Access) Act 2025 (updating, clarifying and simplifying laws regarding data protection and privacy that enables the growth digital services), have been enacted.

3. Trustee responsibilities

Trustee responsibilities are significant in terms the day-to-day operations and governance a pension fund and are governed by Trust and pensions law, the rules the Fund and also data protection law in relation to how Personal Data/information in respect the members and beneficiaries the Fund is held and processed.

Under GDPR, the Trustee of a pension fund is defined as a "Data Controller" as it determines either alone, or jointly with others, the purposes and means by which Personal Data held in respect Fund membership and processed.

Other advisers to the Trustee such as the Actuary, legal advisers, investment managers, and auditors, and also the sponsoring employer and employers who participate in the Fund, may also be classed as "Data Controllers" or "Joint Data Controllers" with the Trustee to the extent that they too determine the purpose and means of processing Personal Data. As Data Controllers they too must hold and process any Personal Data fairly and lawfully.

4. Data Protection Principles

As "Data Controllers", the Trustee must act in accordance with the principles the GDPR, which in summary are:

- Lawfulness, fairness and transparency – Data must be processed lawfully, fairly and in a transparent manner;
- Purpose limitation – Data must be collected for specific, explicit and legitimate purposes, and not further processed in a manner that is inconsistent with those purposes;
- Data minimisation – Data must be processed in a manner that is limited to the relevant information necessary for the purposes the processing;
- Accuracy – Data must be accurate and where necessary kept up to date. Reasonable steps must be taken to ensure it is accurate, or is rectified or erased;
- Storage limitation – Data must be held in a form which permits identification Data Subjects for no longer than is necessary for the purposes for which it is being processed; and
- Integrity and confidentiality – processing must take place in a way that ensures security the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.

5. Definitions of Data

"Personal Data" under GDPR is defined as any information from which individual ("Data Subject") can be identified and includes data held either electronically on a computer system, or in paper format.

"Special Categories of Personal Data" under GDPR covers data relating to health, racial or ethnic origin, religious or philosophical beliefs, a person's sex life, sexual orientation, political affiliations, trade union membership, genetic data (inherited or acquired genetic characteristics about physiology or health) or biometric data (physical, physiological or behavioural characteristics such as facial images or fingerprints).

PART II

6. The Trustee Policy in relation to the Fund

In order to comply with GDPR requirements and carry out its duties in respect the Fund, the Trustee has adopted the formal policy "Trustee policy" set out in this document in relation to obtaining, processing, sharing, storing, retaining and deleting both "Personal Data" and "Special Categories Personal Data" and its security.

Under GDPR the Trustee has a legal obligation to demonstrate accountability and this policy provides a framework which assists in compliance with the relevant law and also demonstrates the practices and processes adopted in relation to the Fund.

This policy relates not only to the Trustee, but also to other parties involved in the running the Fund as delegated by the Trustee in accordance with their powers under the Trust Deed and Rules the Fund and in accordance with pension's legislation.

This policy also includes details of working practices adopted in relation to the conduct the Trustee Board and its proceedings to ensure GDPR compliance.

7. Lawfulness of processing personal data

Under GDPR in order to process Personal Data, the Trustee must have a lawful basis for doing so. Trustee has not taken legal advice in respect the Fund's regular day-to-day processing but has considered the six lawful bases for processing Personal Data, and has determined that for Personal Data to be processed lawfully under the Fund it is relying on:

- fact that the processing is necessary for compliance with a "legal obligation" to which the Trustee is subject; that is, legal obligations under the Trust Deed and Rules the Fund, and pensions legislation,
  and
- To meet a "legitimate interest" of the Trustee or a third party.

When considering legitimate interests, the Trustee took into account that these interests must be balanced against the interests or fundamental rights and freedoms the "Data Subject", (i.e. anyone about whom personal information is held, including members, beneficiaries and potential beneficiaries, that is, Active members, Preserved Members, Pensioners, Spouse's/Civil Partners, Children, Pension Credit members, and Closed records (those who have taken refund, transferred out, died, taken a Trivial/De Minimis/Small Lump Sum, full commutation due to severe ill health, or ceased to be eligible, or paid a children's benefit)).

Trustee carried out assessment and does not consider that processing will prejudice the interests, rights or freedoms the Fund membership.

When special categories of data (such as data in respect health) (**"Special Categories of Personal Data"**) are being processed, the Trustee shall rely on the condition the GDPR which allows Special Categories Data to be processed provided the processing is necessary for the establishment, exercise or defence legal claims. Alternatively, the Data Protection Act 2018 permits the Trustee to process Special Categories Data and data relating to criminal convictions when performing its legal obligations in connection with employment, social security or social protection. The Trustee will rely on whichever these two conditions applies in respect Special Categories Data and data relating to criminal convictions already held by the Fund even if at the time the data was collected the data subject was asked to give consent.

8. Purposes for which data is processed

Trustee in its capacity as "Data Controller" processes data in order to undertake/provide some or all the following:

Establishment a "Data Subjects" eligibility to membership the Fund;

- Maintenance pension records for the Fund membership;
- Calculation pension benefits, lump sums, transfer values and other Fund benefits;
- Payment benefits due to members and their dependants and beneficiaries whilst in service, on leaving service, retirement or death;
- Meeting contracting-out requirements
- Communication with members, and responses to member enquiries;
- Calculation, investment and reconciliation contributions and payment AVCs;
- Insuring member benefits
- production annual Reports and Accounts;
- Other financial reporting and returns
- Annual funding updates,
- Triennial actuarial valuations;
- Other actuarial reporting, certification, calculations and returns
- Purchasing annuities and other insurance contracts;
- Paying benefits, maintaining pension records and taxing benefits
- Reporting to HMRC and the payment of tax;
- investment and monitoring the Fund's assets;
- Managing the Fund's risk;
- Exercising powers and discretions under the Fund;
- Any other duties or responsibilities relating to the administration and governance the Fund.
- Carry out assessments and other studies in relation to the Fund.

Where data is obtained from

Data may be obtained from one or more the following sources:

- the employers who participate in the Fund;
- from appointed processor (such as an administrator);
- the member personally;
- the pension Fund Trustee itself;
- a third party acting on behalf the Trustee,
- a government body such as HM Revenue & Customs (HMRC), National Insurance Contributions Office (NICO), Department Work & Pensions (DWP), Pension Protection Fund (PPF), or the Pensions Regulator (TPR).

9. Categories of parties with whom the Trustee is/might be required to share personal data and the reasons for doing so

Employer – the Sponsoring Employer, Principal and Participating Employers the Fund – in order to maintain the pension records the "Data Subject". Examples data shared are: Dates service and /or membership the Fund, Pensionable Salaries, Pension contributions, contracted out data, pension benefits and other pension related information. Data might also be shared with the participating employers for the purposes it assessing its liabilities to the Fund and undertaking legitimate exercises to seek to manage those liabilities more effectively.

Life Assurer – information about the level benefit cover for the "Data Subject" based on a multiple salary, and other information about the calculation of spouse/civil partners benefits for life assurance purposes.

Administrator – in order to maintain pension records, calculate and pay the benefits due to members, their dependants and beneficiaries.

AVC provider – the provider contracted to invest voluntary contribution monies on behalf the "Data Subject" by the Trustee. Information will be held and processed about the "Data Subject" in relation to any Additional Voluntary Contributions the "Data Subject" pays/paid, the value the fund, type investment/s, type of fund, units held, SMPI information and the options available.

Accounting service providers – data relating to "Data Subjects" used in undertaking accounting functions and the production Funds Reports and Accounts.

Fund Auditor – annual audits are undertaken and Personal Data in relation to the "Data Subject" may be reviewed by external auditors commissioned to undertake the audit by clients.

Pension insurer – where benefits are either partially or fully insured or annuity has been purchased in respect individual pension benefits, and/or the benefit the "Data Subject" is physically paid through the pension Trust or the policies are held in the name the Trustee.

Annuity providers – so that a "Data Subject" may purchase benefits for themselves and their dependants through an annuity provider and personal information is provided in order to set up these arrangements.

Pension Payroll provider – in order to pay the pension benefits the "Data Subject".

Banks and payment clearing houses – Personal Data in respect the "Data Subject" is supplied in order to effect a BACS transfer (the Bankers' Automated Clearing Service) or CHAPS (the Clearing House Automated Payment System) in the UK and/or a payment via banking providers when pensions are being paid overseas.

Covenant advisers – if applicable, in order to assess Fund funding, deficits and demographic trends in relation to the membership the Fund.

Fund Actuary and actuarial advisers – in order to provide actuarial advice to the Trustee, undertake annual funding up dates for the Fund and triennial valuations to assess the value all the Fund benefits and the funding position the Fund, or if a new external Actuary has been appointed.

Investment Manager – for services relating to the pension funds/units held with an Investment Manager.

Investment Consultant – monitors the Fund's investments and provides advice and recommendations to the Trustee in order to formulate investment strategies and help in the achievement long term investment goals.

Legal advisor – in certain circumstances, data may be reviewed by a legal adviser on behalf the Trustee in relation to specific "Data Subjects".

Consultant/Secretary to the Trustee – in relation to reporting to the Trustee or in order to obtain decisions where Trustee discretion is required.

Government and Regulatory bodies he Trustee may also be required to share Personal Data with the following government and regulatory bodies: HMRC, NICO, DWP, PPF, TPR, the Pensions Ombudsman.

Pensions Dashboard – If the Fund is required by legislation to connect to a Pensions Dashboard that is, if it has 100 or more relevant members (active, deferred or Pension Credit members as of the Fund year-end date falling between 1 April 2023 and 31 March 2024) (or opts to connect to a dashboard voluntarily) – member pension information may be shared with and processed via the dashboard ecosystem.

Third parties with whom the administrators may contract

list below shows categories parties with whom the administrators may contract to aid the Trustee as "Data Controller" in the provision services involving either third party processing or potential access to Personal Data:

Mortality screening agencies – automatically each month a mortality screening process is undertaken by a third party for all benefits in payment; automatically each year for preserved pensioners. Personal information about the "Data Subject" is sent to a third party in order to establish whether or not any the Fund membership has died.

Tracing agencies – external agencies are used in order to trace "Data Subjects" with whom formal contact has been lost by the Trustee. In cases where there is uncertainty about a "Data Subject's" continued existence advanced tracing exercise may be used.

Archiving companies – historical data held in paper format is archived and catalogued and held securely with specialist archiving companies.

Banking services – are undertaken by UK regulated banking providers.

Paper record shredding specialists – Personal Data and Special Categories Personal Data in paper format which are no longer required for processing is securely shredded by third party specialists.

10. Data Mapping and Record Keeping

In order to identify the Personal Data it controls, the Trustee has carried out a data mapping and review processing activities exercise, by carrying out due diligence on all its third party service providers and professional advisers, including sponsoring and participating employers the Fund, who process/or have in the past processed Fund Personal Data.

To compile this exercise, third parties were asked to provide detailed information regarding their data processing roles, legal basis, security measures, retention policies, and other GDPR compliance steps. This information is summarised in the Trustee's **Data Protection Procedures Manual**, which includes a register service providers and professional advisers past and present.

Note: The Procedures Manual is maintained separately from this policy and may be updated from time to time to reflect operational changes, without requiring re-approval the core policy.

Additionally, analysis was undertaken the Trustee Board's own Personal Data and with whom it is shared.

11. Third Party service providers and professional advisers data maps

Summaries the results of the data mapping and review processing activities exercise are maintained in the Trustee's **Data Protection Procedures Manual** (Record Processing Activities), which includes data maps for current service providers and professional advisers.

Data Mapping (Record Processing Activities), document details:

a. The name of the service provider/professional adviser
b. The role/function of the service provider
c. Whether the service provider is a "Data Processor" or "Data Controller"
d. The legal basis for processing the data
e. The categories of members "Data Subjects" (Active, Preserved, Pensioners, Spouse's/Civil Partners, Children, Pension Credit members or closed records)
f. The description of the data type either "Personal Data" or "Special Category of Personal Data"
g. The purpose of the processing
h. Where the data is held and data security
i. Data source
j. Whether Personal Data is, has been or will/could be disclosed to third parties
k. Whether the data is anonymised or pseudonymised
l. Whether the data is processed outside the UK and/or European Economic Area (EEA)
m. The time limits for erasure of the different categories of data.

Details former service providers and professional advisers are also included in the Procedures Manual, along with a separate data map for Trustee Board personal data, processed in relation to its statutory and legal duties.

Note: Procedures Manual is maintained separately from this policy and may be updated periodically to reflect operational changes, without requiring re-approval the core policy.

Copies all responses from service providers and advisers, along with links to their Privacy Notices, are stored securely on the CartwrightLive (where available) or within the Fund's GDPR records

12. Trustee policies for fair and transparent processing Data Subject's Rights

Under GDPR Data Subjects are granted numerous rights in respect their Personal Data, including:

Right of access

Data Subjects have a right to access their Personal Data and be advised the purposes the processing, the recipients of the data, and how long it is likely to be held. Where information is held in a country or an international organisation outside the United Kingdom/European Economic Area, the Data Subject can also request to be informed the appropriate safeguards in place.

Trustee policy is to comply with this GDPR requirement.

Right to correction of data

Data Subjects have a right to request the correction of inaccurate Personal Data, or completion any incomplete Personal Data held.

Trustee policy is to arrange correction any inaccurate or incomplete Personal Data in respect the Data Subject.

Right to be forgotten

Data Subjects have a right to request that their Personal Data be erased from the records.

However, the Trustee will need to retain certain Personal Data about Data Subjects in order to be able to fulfil its legal obligation to administer the Fund, in order to comply with the Fund rules, other statutory obligations, to identify the Data Subject, to respond to questions from Data Subjects about their benefits, to calculate or continue to pay any benefits for the Data Subject from the Fund, or to establish, exercise or defend legal claims.

It may be possible in certain exceptional and limited circumstances to erase certain data, however, the Trustee policy is not to erase any Personal Data from a Data Subjects record unless its erasure has no effect on their ability to fulfil legal and statutory obligations as detailed above.

If it is decided some the Data Subject's Personal Data can be erased and the Data Subject's Personal Data is shared with a third party, the Trustee will take reasonable steps to inform other Data Controllers and Data Processors that are processing the Personal Data on its behalf about the Data Subject's request to erase certain data.

If the Data Subject does not agree with the Trustee decision to keep their Personal Data, they will be able to bring a complaint under the Fund's Internal Dispute Resolution Procedure.

Right to the restriction of processing

Data Subjects have a right to restrict processing Personal Data, in circumstances where:

- a Data Subject contests the accuracy the Personal Data;
- the processing is unlawful;
- the Trustee no longer need to process the Personal Data, but the Data Subject needs it for the establishment, exercise, or defence a legal claim; or
- a Data Subject objects to processing that relies on the (i) public interest; or (ii) the Trustee or a third party's legitimate interests, as the lawful processing grounds.
- Where a Data Subject makes a request to restrict processing and Trustee is satisfied that the request falls within the circumstances set out above, such Personal Data will only be processed (with the exception storage):

    - with the Data Subject's consent;
    - for the establishment, exercise or defence a legal claim;
    - for the protection rights another person; or
    - for reasons important public interest.

    Trustee will inform the Data Subject before any data processing restriction is lifted.

Right to receive or transfer Personal Data

(Data Subject Access Requests)

Data Subjects have a right to receive a copy their Personal Data in a structured and easily accessible format (Data Subject Access Request) and to request the transfer it to a third party, where technically feasible.

Trustee as Data Controller, can however limit searches for Data Subjects Personal Data to what is 'reasonable and proportionate'.

Trustee Policy on Timing

Trustee policy is to provide information held relating to the Data Subject within one month receipt the request.

information provided will be that a "**Member Data Report**" from the pension administration system showing all the Personal Data held in respect of the Data Subject.

If the Data Subject requests further information and it is clear what the Data Subject requires, the Trustee will extend this period to **two** months if the request is more complex and involves searching through scanned paper files or archived files or the Trustee receives an increased number requests.

If the Data Subject requests further information and it is unclear what the Data Subject requires, the Trustee can 'stop the clock' until they receive full clarification about the scope of a request (e.g. whether a member wants only benefit data or all correspondence or only data/correspondence regarding a particular matter).

Trustee will request additional information, as necessary, to confirm the identity the Data Subject or any person acting on their behalf.

full operational procedure for handling Data Subject Access Requests is maintained in the **Trustee's Data Protection Procedures Manual**. This manual may be updated periodically to reflect changes in practice, without requiring re-approval the core policy.

Right to object

Data Subjects have a right to object to the processing their Personal Data in certain circumstances, including (but not limited to) for direct marketing purposes, statistical purposes, and processing for the Trustee or a third party's legitimate interests.

If a Data Subject objects, relevant Personal Data shall no longer be processed unless there are:

(i) compelling legitimate grounds for processing that overrides the interests, rights and freedoms the Data Subject; or
(ii) data needs to be processed to establish, exercise or defend legal claims.

Trustee policy is to consider any requests the Data Subject, but as no direct marketing takes place in relation to the administration and governance the Fund and there are legal and legislative obligations and compelling legitimate grounds that override the Data Subjects interests and rights, there will be very limited scope for a Data Subject to object to the processing their Personal Data.

Right not to be subject to automated decision-making

Data Subjects have a right to object to automated decision-making that is, making a decision solely by automated means without any human involvement, and profiling (which means automated processing Personal Data to evaluate certain things about an individual) which has a legal effect on the Data Subject.

However, this right does not apply where the automated decision is necessary for entering into, or performing, a contract between the Data Subject and the Trustee; authorised by EU or UK law that requires safeguards to the Data Subject's rights, freedoms or legitimate interest; or based on the Data Subject's explicit consent.

Trustee policy is not to undertake automated decision making or individual profiling which does not comply with GDPR.

The Trustee has a responsibility to provide any communication, or take any actions, requested by a Data Subject in exercise of the rights referenced above, free of charge, except on the occasion where such requests are unfounded or excessive.

Right to complain about the handling of Personal Data

Data Subjects have a right to complain about the way their Personal Data is handled. Any complaint must be acknowledged within 30 days of receipt and appropriate steps to respond and resolve the complaint must be dealt with as soon as possible.

Trustee policy is to comply with this GDPR requirement and as specified under the Data (Use and Access) Act 2025.

Privacy Notice on fair processing

Whether the Trustee receives Personal Data from the Data Subject directly, or from a third party, the Trustee is responsible for providing a compliant Privacy Notice to the Data Subject about the data that has been collected, is held, or is being processed.

Trustee originally issued a Privacy Notice to all Fund members prior to 25 May 2018, reflecting the requirements the GDPR and their rights; and then again when the Fund administrators changed, effective from 1 March 2024. A further notice was issued to reflect the minor changes under the Data (Use and Access) Act 2025.

Fund's Privacy Notice covers Data Controllers and Joint Data Controllers with the Trustee, in relation to the Fund's Personal Data, although each Data Controller is responsible for its own compliance with Data Protection legislation.

Members for whom an address is not held

Where a current address for a member is not held, the Trustee acknowledge that a Privacy Notice will not have been provided to the member. However, the Trustee is satisfied that the steps taken by the administrator to maintain accurate contact details for members means that all reasonable efforts have been made to issue the Privacy Notice to such members.

current version the Privacy Notice is maintained within the Trustee's **Data Protection Procedures Manual**. This manual is held separately from the core policy and may be updated from time to time to reflect changes in legislation, service provider arrangements, or processing purposes, without requiring re-approval the full policy.

Trustee has put in place a process to keep the Privacy Notices under review and acknowledges that further Privacy Notices will be required in certain circumstances, for example where the purpose processing Personal Data changes (i.e. in the case a buy-out/buy-in where information will be transferred to a new third party not previously linked to the administration and governance the Fund).

Expression of Wishes Form

Trustee notes that where it is provided with information about a member's family and dependants (such as in an Expression Wishes form) it considers that it could seriously impair the purpose for which that data is provided if the Trustee was to send a Privacy Notice to all such family and dependants. As a result, the Trustee has decided not to provide a Privacy Notice to those individuals. In taking that approach the Trustee has considered the rights and interests those individuals and also the fact that Trustee does not ask for Special Categories Personal Data in relation to those individuals.

details provided in the members Expression Wishes forms are recorded and the Expression Wishes forms scanned onto the member's record. Trustee will rely on Article 58 (1) the GDPR, that is, that it is subject to an 'obligation professional secrecy' in relation to the protection the Personal Data which it as Data Controller or the administrators as Data Processors has received in this regard.

Transfer of Data outside the UK and/or EEA

Fund's Personal Data may from time to time be transferred outside the United Kingdom or European Economic Area (EEA), for example, if a Member the Fund transfers benefits to a QROPS outside the UK or EEA, or resides outside the UK or EEA and has pension benefits paid to a Bank outside the UK or EEA. The Trustee policy is to ensure its third party service providers have appropriate safeguards in place when transferring Personal Data outside the UK/EEA.

13. Storage, deletion and retention of personal data

GDPR principles require Personal Data to be kept for no longer than is necessary for the purposes for which it is processed and the data should be limited to that which is required for that purpose.

Trustee considers that its policy for retention and erasure Personal Data must be determined in the context its legal obligations as Trustee the Fund and the fact that pension benefits are paid out over a very long period and that members, former members and their survivors may query a calculation or entitlement to benefits many years after settlement the benefit. Trustee is also under a legal obligation to retain certain data for a number years, and this includes HMRC requirements. As a result, the Trustee policy is to keep the majority Personal Data indefinitely.

Trustee has reviewed the contractual terms and considered data retention in relation to each its outsourced service providers, professional advisers, and Joint Data Controllers. A summary these arrangements is maintained in the **Trustee's Data Protection Procedures Manual,** which includes a register current and former service providers and their respective retention policies.

Note: The Procedures Manual is maintained separately from this policy and may be updated from time to time to reflect operational changes, without requiring re-approval the core policy.

14. Data used for pension administration services – On appointment

At take on Buccleuch Estates Limited 1974 Retirement Fund all Personal Data held electronically by the previous administrators (Mercer) was migrated onto the pension administration system used by the new administrators.

Where the previous administrators supplied historical pension correspondence in electronic format this was uploaded onto the pension administration system, or, if it is was in paper format it was also scanned onto the members electronic records on the pension administration system.

On-going processing

Transfers out/Trivial Commutations/De Minimis/Small Lump Sum payments.

If a member fully extinguishes all liability to benefits under the Fund, the pension administration system will be updated with full details where the benefit has been transferred/paid, the amount the payment, the date paid, and any tax deducted if applicable.

All correspondence relating to the payment will be scanned onto the member record or held in a member's personal record on the pension administration system.

member record will be held as a "closed" record on the pension administration system indefinitely.

Deceased Member records

If a member dies and all liability for benefits under the Fund has been extinguished (i.e. there are no surviving dependants entitled to a benefit from the Fund and any death benefits due have been distributed, or unpaid benefit payments made to the estate), the pension administration system will be updated with full details the death.

All correspondence relating to the death and payments made will be scanned onto the member record on the pension administration system.

member record will be held as a "closed" record on the pension administration system indefinitely.

General policy on "closed" records

All "closed" records will continue to be held on the pension administration system indefinitely.

All scanned correspondence on the pension administration system will continue to be held indefinitely.

Cartwright will only use retained data for "closed" records for the following reasons:

- Guaranteed Minimum Pension reconciliation exercises;
- Guaranteed Minimum Pension equalisation exercises;
- Audit purposes;
- The purposes answering queries at a future date;
- Undertaking benefit audits;
- Undertaking membership reconciliations;
- Undertaking actuarial valuations;
- Trustee defending itself against a former member or litigation relating to the Fund or to ensure compliance with local law and regulatory requirements.

If Cartwright does not provide **all** administrative services data will be held as specified in the Data Map (Record Processing Activities) document. Buy Out/Wind up

If the Fund were to buy out all its liabilities with an insurance company or wind up and all member benefit liabilities are fully extinguished, each member record on the pension administration system will be updated with full details any trivial commutation, winding up lump sums, or De Minimis/ Small Lump Sums paid, and details where the benefit has been transferred and that no further liability exists under the Fund.

If Cartwright were the Fund administrators before buyout/wind up, all member correspondence relating to the buyout /wind up will be scanned onto the member record on the pension administration system.

Buy Out/Wind up retention/destruction policy

member data on the pension administration system will be held as a "closed" record and any member personal correspondence scanned on the member record on the system will be held for a period seven years only and then deleted.

Cartwright will offer the Trustee the opportunity taking extract the all the member data and any correspondence held electronically, subject to the completion a formal Transfer Information Agreement signed by all relevant parties (the Trustee and Cartwright). Transfer Information Agreement will state that in the event a claim or litigation, Cartwright will be permitted access to the data/documents or parts thereof in order to defend themselves.

If the administrator is not Cartwright or does not have a scanning facility the personal member file will be archived and held for a period seven years and then destroyed or retained in accordance with any specific agreement made between the former service providers and the Trustee.

15. Data used for accounting purposes

Buccleuch Estates Limited provides the accounting services for the Fund and produces the Report and Accounts. Data will be held as specified in the Data Map (Record Processing Activities) document.

All Personal Data used in the day to day accounting functions and in relation to the production the Report and Accounts and submission tax returns is to be retained indefinitely.

16. Data used for pension payroll services

Buccleuch Estates Limited provides the pension payroll services for the Fund. Data will be held as specified in the Data Map (Record Processing Activities) document. All Personal Data used in relation to the day to day payroll functions including RTI submissions, end year returns and tax returns is to be retained indefinitely.

17. Data used for actuarial services

data used in order to undertake annual funding updates for the Fund and triennial valuations to assess the value all the Fund benefits and the funding position the Fund is provided by the administrators to the Actuary.

data held by the Actuary will be restricted to the minimum required to undertake the actuarial functions. If Cartwright is the Actuary the data will be held for four years (3 years for the valuation period +1 year) until the next Triennial Valuation is completed and signed off, and then destroyed.

Data used for the calculation other benefits such as transfers out, trivial commutations, early retirements, late retirements, special augmentations, pension debits/credits, "Scheme Pays" deductions will be held as follows;

For quotations that do not proceed – for a period 13 months (12 months + 1 month for transfer value quotation purposes). For quotations that go ahead as proof the calculation, the data will be held indefinitely.

18. Transfer of services to a new provider/ professional adviser

If the Trustee decides to terminate or transfer all or any the services undertaken by Cartwright (administration, consultancy/secretarial services, and investment consultancy services) relating to the Fund to alternative provider, or appoint a new Actuary other than a Cartwright Actuary or terminate any services, Cartwright will retain archive copy the data which will only be accessed in the event and to investigate and defend a claim against Cartwright.

policies adopted in relation to other third-party service providers and professional advisers are summarised in the Trustee's **Data Protection Procedures Manual**, which includes the Data Map (Record Processing Activities). This manual is maintained separately from the core policy and may be updated from time to time to reflect operational changes, without requiring re-approval the policy itself.

19. Former service providers and professional advisers

Trustee contacts all recently retired trustee directors in order to inform them the requirements the GDPR and to ask them to return or securely destroy any Fund Personal Data which they still hold.

Also, all known former service providers and professional advisers have been contacted in relation to the Personal Data they may still hold in relation to the Fund.

Both the Trustee and the Fund's administrator shall review the Fund Personal Data they hold to ensure that it is limited to what is necessary, and that there are suitable processes in place for verifying data accuracy, taking into account guidance of the Pensions Regulator and for correcting/deleting inaccurate data.

Responses from the former service providers and professional advisers are summarised in the Trustee's **Data Protection Procedures Manual**.

20. Security of Processing – where Cartwright has been appointed to undertake consultancy/ secretarial services

Trustee is aware the standard security and appropriate technical and organisational measures required under the GDPR. The Trustee has taken into account factors such as the costs implementation that security, the nature, scope, context and purposes processing and the risk the varying likelihood and severity for the rights and freedoms Data Subjects to ensure a level security appropriate to such risk in respect its processing Fund Personal Data.

In particular, the Trustee has put in place the following measures:

- Fund Member Reference Number only

Wherever possible, papers and materials circulated to/from the Trustee and the Trustee advisers that contain Personal Data will not contain the name the Data Subject, but will contain the Fund member reference number only.

- Exercising discretion to pay Defined Benefit Death Benefit Lump Sums

Papers and materials containing Personal Data about a Data Subjects family in the event that the Trustee needs to exercise discretion regarding the distribution a Defined Benefit Death Benefit Lump Sum will be anonymised where possible.

- Ill health retirements

Papers and materials containing Personal Data about a Data Subject who qualifies for retirement on ill health grounds/serious ill health grounds for which the Trustee needs to confirm their opinion that the Data Subject meets the ill-health criteria, will be anonymised where possible.

- Administration Management Reports and other Trustee reports, papers and materials

Consultant/Secretary will provide additional information about the anonymised members (Data Subjects) quoted in Administration Management Reports and other reports, papers, and materials to the Trustee in order they may identify the Data Subjects using a key to the Data Subjects name and other relevant information and provide this to the Trustee if required at the Trustee Board meeting.

- Documents with the key to the anonymised data

These documents containing the additional member information will be stored on the Fund files/CartwrightLive under the Cartwright secure network after the meeting has taken place and will be held indefinitely.

- Trustee Minutes

Trustee Minutes which detail discretionary decisions taken, particularly those affecting member's (Data Subjects) benefits or entitlements or benefit treatment, will be restricted to:

1. Listing the factors taken into account by the Trustee in coming to their decision, and
2. Summarising briefly the advice received by the Trustee, and
3. Recording the decision taken without any particular or specific reason being given for the decision taken or details the Trustee.

decision will be noted on the Data Subjects' member record or personal file and the Data Subject, and any other interested parties, will then be informed the decision, with reasons given.

- Password protection, end to end encryption, or Secure mail

All papers and materials circulated to/from the Trustee and their advisers which contain Personal Data will be sent via Mimecast and if not must be password protected, sent via end to end encryption or issued via Secure Mail.

- Cartwright Secure Network

Where possible all papers and materials will be held on the Fund file or CartwrightLive under the Cartwright secure network.

- Trustee Meeting Packs

All hard copy Trustee meeting packs and notes made at meetings will be securely stored by the Trustee or destroyed by the Trustee once the meeting minutes have been circulated to all the Trustee Board, all amendments made, and they are ready for signature.

21. The Working Practices of the Trustee

In addition to the policies detailed above, the Trustee has adopted specific working practices to support the administration and governance the Fund and ensure GDPR compliance. These practices are maintained in the Trustee's Data Protection Procedures Manual, which includes operational guidance and templates used in day-to-day activities.

Note: The Procedures Manual is maintained separately from this policy and may be updated from time to time to reflect changes in practice or service provider arrangements, without requiring re-approval the core policy.

This approach ensures flexibility in updating operational procedures while preserving the integrity the Trustee's formal data protection policy.

22. Cyber Incidents and Data Breaches

Trustee recognises the authority the Information Commissioner (formerly the "ICO") and it intends to cooperate on request with the IC. Trustee recognises its obligation to inform the IC certain data breaches within 72 hours becoming aware them, unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms Data Subjects.

Trustee will consider cyber and data protection risks as part the ORA, ensuring that breach management, resilience testing, and supplier assurances are explicitly assessed and documented within the ORA cycle.

Trustee has a separate policy on IT Cyber Controls and Cyber Security and undertakes a Cyber Risk Assessment to comply with the Pensions Regulator's guidance. It also maintains a Cyber Incident and Data Breach Response Plan, which sets out how each case will be assessed and managed individually should a breach occur.

Cyber Incident and Data Breach Response Plan is maintained within the Trustee's Data Protection Procedures Manual and may be updated from time to time to reflect operational changes, without requiring re-approval the core policy.

23. Children

Trustee acknowledges that under GDPR, processing data relating to children needs consent the holder parental responsibility over the child if they are under the age 13 years. Trustee policy is therefore, to communicate only with the parent or guardian the child, if the child is under the age 13 years. If the child is over the age 13 years, and although not considered to be an adult under UK law, it will communicate directly with the child in relation to their educational status and in relation to any benefits they may receive from the Fund.

24. Ill-health

Trustee acknowledges that under GDPR, data relating to a member's health is categorised as a "Special Category Personal Data" and processing that data can generally only take place with the explicit consent the member. In the case ill health retirements data may therefore be held covering the following type information:

- Employer/Trustee consent to ill-health retirement;
- Details any increased benefits,
- Doctor's /consultants/health care professionals name and address;
- name and address the hospital a member may attend;
- nature the illness including diagnosis and prognosis;
- Details a member's medication;
- Frequency review and;
- Review date

Although the Rules permit the payment enhanced early retirement pension on grounds ill health and prior to the member reaching Normal Retirement Date, the Trustee has a discretion to require a Member who has retired on grounds incapacity to ask for evidence his continued incapacity and the amount his earnings, and may suspend or reduce the pension if there is evidence there has been an improvement in their health, there are no recorded ill health cases under e Fund.

In the event a future ill health case occurring consent to processing will be received in advance the case being considered and put into payment.

25. Cyber Security – Data Security Measures – where Cartwright has been appointed to undertake services

Data Security concerns the protection data from accidental or intentional but unauthorised modification, destruction or disclosure through the use organisational, people, physical and technological controls to provide assurance that information and other associated asset are kept reasonably secure and protected against threats and harm.

Detailed below is a description the controls in place at Cartwright to ensure that Personal and Special Categories of Personal Data is kept secure.

The security and encryption of Personal Data

All data sent externally by Cartwright to third parties will be sent securely/encrypted.

For security reasons, no correspondence is sent to a "Data Subject" in which Cartwright includes details their National Insurance Number. This measure has been put in place to help in the prevention fraud as it reduces the risk a "Data Subject" being identified from stolen or lost correspondence.

Data Transfer – Secure mail/password protection

transfer all Personal Data undertaken by email is sent securely via Secure Mail (Mimecast) or is password protected. (Secure Mail is a secure, private service that enables the sharing information with external contacts via a secure web portal).

Data Transfer – Secure File Transfer Protocol (SFTP)

Substantially large data sets are transferred via Secure File Transfer Protocol, and transfers are further restricted via Internet Protocol (IP) address, which allows control over who has access to the secure site.

Transfer of data between internal systems

Data transferred between systems, for example from the administration system to the actuarial system(s), is kept to the minimum. The following information will be excluded from any data transferred to the actuarial system(s):

Member National Insurance number, member name, title and initials, member marital status.

Only the Fund name, the member reference number, and the member category, will be used as an identifier.

only exceptions to this will be if there is a specific case where an individual's benefits require specific calculation by the Actuary.

Trustee acknowledges therefore that as all the Cartwright internal systems sit within the same secure environment, there is no transfer outside the secure system when data is transferred, for example, from the administration system to the actuarial system.

Ongoing confidentiality integrity availability and resilience of processing systems and services – Cyber Security:

Measures Cartwright have in place

- State- -the-art Vulnerability management tools are deployed to identify vulnerabilities across devices and automatically update or patch software.
- Single Sign On and multi factor authenticated network access for prevention malicious network access.

- Anti-virus protection from the latest email based threats including:
    - Whaling (targeted executive fraud).
    - Spear-phishing (impersonation to obtain special category or private information).
    - On-click protection from malicious URL's (Uniform Resource Locators) in emails (prevents the introduction malware/viruses to our network via clicking on malicious URL's within emails).
    - Attachment sandboxing (scanning for malicious content before it is introduced onto the Cartwright network).
    - Email encryption (security of email in-transit and at rest
    - Real-time protection against outbound data leaks with automated policy application (prevention emails sent insecurely).
- Encrypted off site backups and server replication (allowing quick and responsive reinstatement data and systems in the event a disaster or network breach).
- User Privilege Management (to ensure internal data access is only permitted to those that have a need to access it).
- Real time Virus scanning – up to date virus definitions to recognise malicious behaviour and prevent its application.
- Device encryption – prevention unauthorised plug and play devices (laptops, USB Sticks, mobile phone remote swipe etc.).
- Processes for regularly testing assessing and evaluating the effectiveness security measures.

Cartwright adheres to approved code conduct and certification mechanism to demonstrate compliance with GDPR and the effectiveness the security measures it has in place.

Cartwright operates Information Security Management System that aligns with Cyber Essentials, the UK Government's minimum baseline standard for cyber security requirements and the internationally recognised standard for Information security, cybersecurity and privacy protection ISO/IEC 27001.

26. Cyber Security – Data Security Measures – other service providers/professional advisers

Trustee has received confirmation from all third party service providers and professional advisers that appropriate cyber security protections in place, and any security issues identified have been added to the Fund's risk register.

Trustee is satisfied that at the date this policy, all third party service providers and professional advisers meets the security processing requirements set out under the GDPR, but shall keep such measures under ongoing review.

27. Data Protection Impact Assessment ("DPIA")

Trustee acknowledges that in addition to having completed a full assessment all service providers and undertaken a full Data Map (Record Processing Activities) exercise to create this policy that a DPIA will be required whenever there is a change in the technologies used by, or a change in any third party service provider or professional adviser.

This will be added to the Fund's Business Plan and Risk Register and will be reviewed by the Trustee periodically to obtain confirmation that there have been no changes that affect compliance with GDPR.

28. Appointing new service providers or professional adviser

On appointment new individuals or organisations to assist the Trustee with the administration and governance the Fund, the Trustee will require them to provide a written statement compliance with GDPR and the Trustee specific requirements for data processing, data security, data retention and destruction, Data Subject Access Requests and consent, in accordance with this policy.

29. Data Protection Officer

Trustee is not required to appoint a Data Protection Officer under Data Protection legislation as it is not a public sector organisation and its core activities do not require the regular and systematic monitoring Data Subjects on a large scale, nor the processing special category data relating to criminal convictions and offences. Therefore it has not appointed one. However, it has received guidance from the company's internal Data Protection representative at dataprotection@buccleuch.com and its professional advisors, to assist it in meeting its responsibilities and comply with GDPR as detailed in this policy document.

30. Review of Policy

Trustee reserves the right to amend this policy from time to time and will undertake a regular review the decisions and practices set out herein. Where necessary, including in response to updated guidance from the Information Commissioner or changes in legislation, the Trustee will issue a revised policy.

Trustee will also review all related documentation—such as data sharing agreements and contractual terms with advisers and service providers—to ensure continued compliance with data protection requirements.

This policy forms part the Trustee's integrated risk management framework. GDPR compliance, data security arrangements, and supplier oversight will be considered as part the Trustee's Own Risk Assessment (ORA), undertaken in line with the Pensions Regulator's General Code Practice.

ORA will document the Trustee's assessment data protection and cyber security risks, the adequacy current controls, and any remediation actions required. Findings from the ORA will inform updates to this policy and to the Trustee's Risk Register.

To embed regular oversight, this policy has been added to the Trustee Board's Risk Register and Business Plan. It will be reviewed:

- Annually as part the Trustee's governance cycle;
- On appointment any new third-party adviser or service provider;
- On adoption any new system or technology; and
- Following any material legislative or regulatory change affecting the processing Personal Data.

Date Policy Adopted: 12 November 2025

Lord Damian Scott ..... Signed by: Lord Damian Scott 82310A0BF23F4C8...

The Earl of Dalkeith ..... Signed by: Walter Dalkeith 1FE5C95832AC422...

Kathryn Barclay ..... Signed by: Kathryn Barclay 0F4073C0EC75444...

John Webster ..... DocuSigned by: 6EEDF1E1237C4C4...

Date of last review: 12 November 2025