

UCAS Pension and Life Assurance Scheme (1993)

Annual Review of General Data Protection Regulation (GDPR) Policy

Following the introduction of the revised GDPR requirements with effect from May 2018, it was agreed that the Trustees would review their policy and the Fair Processing Notice issued to members on an annual basis.

The attached policy and Fair Processing Notice show the most recent versions of each document for consideration at the May 2019 meeting.

UCAS Pension & Life Assurance Scheme (1993)

Data Protection, Privacy and Information Security Policy

1 INTRODUCTION

In the ordinary course of administering and managing the UCAS Pension & Life Assurance Scheme (1993) (the "**Scheme**") the Trustees collect, hold, process and transfer personal data relating to members of the Scheme ("**Members**") and other beneficiaries in receipt of benefits from the Scheme such as Members' dependants ("**Beneficiaries**").

The Trustees recognise the importance of establishing and operating a very high standard of data protection for personal data, as failure to do so can have serious legal implications and may, from 25 May 2018 for certain breaches of European Data Protection Legislation, result in the imposition of a fine of the higher of 4% of annual global turnover of the sponsoring employer and €20 million¹

The Trustees are the data controller (as defined under European Data Protection Legislation) for any information that it collects from Members and Beneficiaries in connection with administering the Scheme. This Data Protection, Privacy and Information Security Policy (the "**Policy**") relates to the handling and processing of all Members' and Beneficiaries' personal data, whether held manually or electronically, and sets out the minimum standards of conduct and procedure the Trustees expect for the handling of Members' personal data in compliance with the European Data Protection Legislation. The Scheme Actuary is a joint data controller with the Trustees and other parties may be data controllers for certain tasks.

2 DEFINITIONS

For the purposes of this Policy, "European Data Protection Legislation" is defined as, for the periods in which they are in force, the European Data Protection Directive 95/46/EC, all laws giving effect or purporting to give effect to the European Data Protection Directive 95/46/EC (such as the Data Protection Act 1998) or otherwise relating to data protection (to the extent the same apply) and, from 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) or any equivalent legislation amending or replacing the GDPR.

3 SCOPE

3.1 Who does this Policy apply to?

Anyone that processes (i.e. collects, stores, uses, transfers, discloses etc) personal data controlled by the Trustees, therefore all individual Trustees. The Trustees will also have regard to this Policy in their dealings with their advisers, suppliers, the Scheme's sponsoring employer and other third parties including but not limited to other companies in the sponsoring employer's group.

Failure to adhere to this Policy may result in civil or criminal legal action being taken against the Trustees by data protection authorities or by the individuals to whom the personal data relates.

3.2 What does the Policy relate to?

The processing of Member personal data. Processing means:

- carrying out any operation or set of operations on the data;
- collecting, recording or holding data; and
- use of the data which includes but is not limited to transferring, amending, consulting, sharing, storing, archiving and even destroying it.

3.3 What is Member personal data?

Any information relating to a Member or Beneficiary from which such Member or Beneficiary can be identified, directly or indirectly, or from which, with other information, they can be identified. These identifiers may include the Member's name, address, date of birth, an identification number such as a National Insurance number, health data, an online identifier or one or more factors specific to the physical, psychological, mental, economic, cultural or social identity of that Member.

It makes no difference where the data is held, e.g. whether it is in a computer database, on e-mails, or on paper in a filing system of such a type that the data is readily obtainable.

4 CORE PRINCIPLES OF THIS POLICY

4.1 Data Protection Laws

It is essential that each individual Trustee:

- complies with this Policy;

- understands and observes any data protection laws applicable, including the European Data Protection Legislation, and
- ensures that Members' and Beneficiaries' personal data is handled with appropriate confidentiality and security.

4.2 Collection and Use of Personal Data

The Trustees collect personal data in many ways including but not limited to from Members and Beneficiaries (or their IFA) directly; from application forms completed by Members on joining the Scheme; from a Member's employer; from expression of wish forms completed by the Member; from information provided in relation to potential beneficiaries on the death of a Member, from track and trace services and from HMRC and other law enforcement agencies. The data is collected and processed for the purpose of:

- calculating and paying benefits;
- administering the Scheme;
- managing the Scheme (as a whole and Members' membership of it) by the Trustees and any third party to whom the Trustees have delegated obligations arising in connection with Members' and Beneficiaries' benefits;
- carrying out obligations arising from any contracts entered into between Members and their employer and to provide Members with any information they request from the Trustees;
- analysis by the Trustees and, to the extent necessary, any other organisation required (such as the Trustees external advisors, including legal advisers, and the Trustees' insurers or potential insurers);
- communicating with Members and Beneficiaries about their pension by mail, telephone, email, text or other electronic means;
- complying with the Trustees' auditing and/or reporting requirements;
- complying with legal and regulatory requirements or to protect the rights, property or safety of the Trustees, the Members and Beneficiaries, or others; and
- complying with the Trustees' legal obligations, resolving disputes and enforcing the Trustees' rights.

The underlying principles for the collection and use of personal data are that:

- it should be processed fairly and lawfully. Personal data will be collected and processed only for legitimate needs relating to the Scheme, used only for purposes that are known to the Members and Beneficiaries, and kept confidential. Where data is to be disclosed to a third party outside the Scheme, or transferred outside the European Economic Area (“EEA”), Members should be made aware of this.
- it should be adequate, relevant, and not excessive. No more data should be gathered than is needed - personal data should not be gathered or held "just in case".
- it should be accurate and kept up to date. Personal data should be correctly recorded, and updated promptly when appropriate. Procedures and control must be in place to ensure that this is achieved.
- it should be kept no longer than necessary, or as required by law.

4.3 Rights of the Individual

It is the Trustees' policy to respect the rights of Members and Beneficiaries and to provide them with reasonable access to data held.

The Trustees will provide Members and Beneficiaries with written information about the data it controls and how they should exercise their rights in relation to it through issuing them with a Fair Processing Notice. The Trustees issued an updated Fair Processing Notice to all Members and Beneficiaries prior to 25 May 2018 and will re-issue such notices where appropriate e.g. if they wish to share personal data with a new third party. The Trustees acknowledge that they may also control personal data in relation to certain former Members of the Scheme (e.g. those who have transferred their benefits from the Scheme) but as they can no longer be certain that they hold up-to-date addresses for such persons, they have decided it would be disproportionate to send Fair Processing Notices to them.

At their written request, Members and Beneficiaries will be provided with a copy of their personal data held by the Trustees unless any such data can be legitimately withheld. Up until 25 May 2018, a fee of £10 may be charged for this. After that date the Trustees may request a fee only where appropriate in accordance with the European Data Protection Legislation, for example, if the requests are manifestly unfounded or excessive, in particular because of their repetitive character.

If necessary the Member or Beneficiary making the request may be asked to prove his/her identity and may also be asked to provide information to enable the data in question to be located. The information should be provided as soon as is practicable and in any event

within 30 days of the Member or Beneficiary making the request although this can be extended by a further 2 months if the request is particularly complex or a large number of requests are received by the Trustees.

Furthermore, at their written request, the information can be provided to Members and Beneficiaries in a way that makes it easy for a computer to read.

Members and Beneficiaries should be permitted to correct or update the information as necessary.

Members and Beneficiaries also have the right to ask the Trustees to delete or remove any personal data they hold in relation to them if:

- the personal data is no longer necessary for the administration and management of the Scheme;
- they have withdrawn their consent to processing and consent was the only legal basis on which the Trustees were entitled to process the data (e.g. potentially in relation to the processing of health data where the Trustees have no other lawful basis for processing such data);
- they have objected to the processing and there is no overriding legitimate interest for continuing the processing.

The Trustees can refuse a request from a Member or Beneficiary for his data to be deleted where the data is required to comply with a legal obligation e.g. in case of enquiries from HMRC or where it may be needed for the exercise or defence of legal claims. If the Trustees are unsure as to whether they should comply with such a request they should seek legal advice.

4.4 Special Categories of Personal Data

Special categories of personal data (formerly known as sensitive data) is information on a Member's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, physical or mental health, data concerning health or sex life and sexual orientation, criminal convictions and offences or related security measures that is not carried out under the control of official authority, genetic data and biometric data.

The collection and processing of special categories of personal data is very strictly regulated generally requiring the freely given, specific, informed and unambiguous consent of Members and Beneficiaries (unless processing is necessary to carry out the

Trustees' legitimate interests, for example, to make a determination in connection with a Member or Beneficiary's eligibility for benefits payable under the Scheme and even then only where the Trustees have an enforceable data protection policy which sets out how such data is retained and erased).

It is the Trustees policy to collect special categories of personal data only when absolutely necessary, for example, when considering an application for an ill-health early retirement pension or determining eligibility for a lump sum or spouse's pension following a Member's death.

Special categories of personal data must be made available to users only on a strict "need to know" basis, and managed with the highest practical level of security and confidentiality. For details of the Trustees' security and confidentiality measures, see section 5 below.

4.5 Disclosure of Personal Data

It is the Trustees' policy to ensure that personal data relating to Members and Beneficiaries is protected at all times, and it is the responsibility of all users of personal data to ensure that data is treated confidentially. The Trustees may share Members' and Beneficiaries' personal data with the Member's employer, other participating employers in the employer group, other companies in the employer's group, the scheme administrator and the Trustees' professional advisors and service providers to the extent that it is necessary for the management and administration of the benefits provided by the Scheme.

The Trustees may share Members and Beneficiaries' personal data with selected third parties including but not limited to:

- when specifically asked to do so by the Member or the Beneficiary e.g. to an independent financial adviser;
- in the event that the sponsoring employer sells or buys any business or assets, in which case the Trustees may disclose Members' or Beneficiaries' personal data to the prospective seller or buyer of such business or assets and their advisors;
- in the event that the Trustees consider de-risking or insuring any of the benefits provided by the Scheme in which case the Trustees may disclose Members' or Beneficiaries' personal data to prospective insurers and/or its or the sponsoring employer's advisers;

- if the Trustees are under a duty to disclose or share Members' and Beneficiaries' personal data in order to comply with any legal obligation or to protect the rights, property or safety of the Trustees, or others. This may include exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

The Trustees do not use Members and Beneficiaries' personal data for marketing purposes or transfer personal data to other organisations for the purpose of marketing their goods or services.

When the Trustees share personal data with third parties, such third party will process Members or Beneficiaries' data as either a data controller or as the Trustees' data processor and this will depend on the purpose of the Trustees' sharing of the data.

Where personal data is disclosed to third parties who will be processing data controlled by the Trustees it must be done so in accordance with European Data Protection Legislation. In such circumstances:

- the Trustees must ensure that third parties are reliable, that they will keep data confidential, and that they have adequate technical and organisational security arrangements in place;
- a contract must be in place that binds the third party to the same obligations as apply to the Trustees, and under which the third party agrees to act only in accordance with instructions from the Trustees, and to take adequate technical and organisational security measures when processing personal data; and
- no more data should be provided than is necessary for the performance of the contract.

The personal data that the Trustees collect from Members and Beneficiaries may be transferred to, and stored at, a destination outside the EEA to the extent that it is necessary for the management and administration of the benefits provided by the Scheme. It may also be processed outside the EEA by the Trustees' advisers or suppliers. In compliance with the European Data Protection Legislation, should Members' and Beneficiaries' personal data be transferred to, and stored at, a destination outside the EEA the Trustees will take all steps reasonably necessary to ensure that such data is safeguarded through adequate means, such as ensuring that the recipient has entered into Standard Contractual Clauses approved by the European Commission.

Those who process data controlled by the Trustees are:

Barnett Waddingham LLP as Scheme Administrator;

Burges Salmon LLP as legal advisers to the Scheme;

Nexia Smith & Williamson Audit Limited as independent auditor to the Scheme

The Equitable Life Assurance Society as AVC provider;

Clerical Medical Investment Group Limited as AVC provider

The Trustees have confirmed that its sharing of personal data with its data processors complies with the requirements set out in this section 4.5 and in section 4.6 below.

In addition, the Trustees' advisers include the following who are data controllers in their own right and will, therefore, be directly responsible for complying with European Data Protection Legislation when processing any personal data relating to the Scheme's Members and Beneficiaries:

Susanna Morran of Barnett Waddingham LLP as scheme actuary is a joint data controller with the Trustees;

Burges Salmon LLP as legal advisers to the Scheme;

Other parties may be data controllers for certain tasks.

Again, the Trustees have confirmed that their sharing of personal data with such third parties complies with the requirements set out in this section 4.5 and in section 4.6 below.

4.6 Data Security

The Trustees ensure that risk appropriate technical and organisational measures are in place to prevent unauthorised or unlawful processing and accidental loss, disclosure, destruction, damage or access to personal data, whether in the Trustees' possession or in the possession of third parties. Please see section 5 of the actions the Trustees take to ensure the security of Members and Beneficiaries' personal data when in its possession.

The Trustees will also take reasonable steps to safeguard the accuracy and completeness of personal data, whether in the Trustees' possession or in the possession of third parties.

The Trustees ensure that data processors use, adopt and continue to comply with appropriate technical and organisational security measures. The Trustees ensure that:

- they are satisfied that data processors are clear about their responsibilities and that they have been provided with any written policies on the data processors' record keeping processes;

- they are clear about what data processors will, and will not, do for it and what information they need from it;
- they are satisfied that any information they need from data processors is readily available so that they can meet their other legal and regulatory responsibilities;
- they inform data processors promptly about any changes in order that they can keep their records up to date;
- they are satisfied that they are kept informed of any problems data processors encounter with maintaining scheme records, or would be kept informed if any were to arise;
- any personal data sent by data processors to Trustees is encrypted, anonymised or pseudonymised; and
- records are kept on the systems of the Scheme's administrator from time to time for as long as it takes to provide the pension and other benefits provided under the rules of the Scheme and for such period afterwards as necessary to comply with the Trustees' legal obligations, resolve disputes and enforce its rights.

5 TRUSTEES PRACTICE TO ENSURE SECURITY OF PERSONAL DATA

Each individual Trustee will comply with the following technical and organisational measures to aim to prevent the unauthorised or unlawful processing and accidental loss, disclosure, destruction, damage or access to personal data. The golden rule is to respect the privacy of the Members and the Beneficiaries to whom the data relates and to treat their data as highly confidential. This means that each individual Trustee will:

- comply with this Policy in all respects at all times;
- only record information which is necessary and not use it for purposes which have not been communicated to Members and Beneficiaries in the Trustees' Fair Processing Notice;
- not provide information unless it is certain the recipient is who they say they are and that they have a valid justification for receiving the data;
- provide only the data necessary to fulfil the purpose for which it is required by the recipient;
- not provide information over the telephone, fax, or in any other way, if the Trustees are not certain who will receive it. If in doubt, the Trustees will not give the information;

- ensure that the Trustees have explicit consent to process special category personal data or that they have another lawful basis for processing such data; and
- ensure that special category personal data is kept even more securely, with access strictly limited, and used only for the approved purpose. The Trustees will not collect such data unless it is essential to do so.

The only personal data relating to Members and Beneficiaries that each individual Trustee has access to:

- relates to individual Member cases (e.g. relating to death or ill-health cases) which the scheme administrator sends to the Trustees via a link to its secure encrypted website;
- is contained within meeting papers issued by the scheme administrator as part of the electronic meeting pack sent via a link to its secure encrypted website

Elementary housekeeping to ensure the security and confidentiality of such personal data is vital. In particular each individual Trustee will:

- ensure that access to any personal data stored electronically is password protected, and keep passwords confidential;
- ensure that manual data and files are secure at all times, for example in a locked filing cabinet or locked drawer;
- not leave information unattended, whether paper records or unattended computer screens;
- ensure that personal data records are accurate and up-to-date, and that unnecessary and outdated records are deleted/destroyed;
- not print personal data if it is not essential to do so, and ensure that printouts are shredded and disposed of properly when no longer needed. In particular, the Trustees will ensure they do not keep any hard copies of individual Member cases or of any meeting packs at home and will shred or return any such material to the scheme administrator once the individual case has been considered or once they have reviewed and provided comments upon the minutes of any Trustees meeting;
- not forward or share any materials containing personal data except to the Trustees' advisers, other Trustees or to reply to the sender of the email;

- delete emails containing personal data (along with any attachments) as soon as they have been actioned;
- if available use a company email address for Trustee business and access their emails via a securely protected mobile phone, tablet or personal computer. not allow anyone else access to their email account (including family members and other Trustees although the Trustees may use the same email address for Trustees' business as for other purposes; Alternatively, access scheme documents via the secure file exchange provided by the Scheme Administrator.
- take appropriate measures to ensure the security of their mobile phone, tablet or personal computer as the case may be. In particular, each Trustee will ensure that such devices are password-protected and consider functionality to remotely wipe data if a device is lost or stolen;
- before accessing personal data from outside the EEA, consider whether such access is really necessary.

If any Trustee has any queries regarding how to ensure the security of their systems, they should speak to the sponsoring employer's IT Department.

6 DELETION AND DESTRUCTION OF DOCUMENTS

The Trustees will consider, on a regular basis, whether it is necessary to retain certain records. In doing so, the Trustees recognise that pensions are long-term investment vehicles and it is not uncommon for queries or disputes to arise in relation to Members' and Beneficiaries' benefits years after a Member has left the service of his employer or even after a pension has been put into payment. As a general rule, therefore, records relating to the calculation of Members' and Beneficiaries' benefits along with records relating to Members who have transferred their benefits out of the Scheme will be retained for 6 years following the winding-up of the Scheme.

Each Trustee will ensure they do not keep any hard copies of personal data at home and will shred or return any such material to the scheme administrator once the individual case has been considered. Where hard copies of personal data are to be destroyed, the Trustees will always use a shredder or confidential waste bag.

If any Trustee has any doubt as to whether it is appropriate to delete or destroy a particular document, they will ask the Chairman of Trustees who will decide the appropriate course of action.

7 REPORTING BREACHES

Breaches of this Policy, whether actual or suspected, must be reported by individual Trustees to the Chair of Trustees or, in his absence, to a person designated by the Chair of Trustees to receive such reports, within 48 hours of becoming aware of a breach. The Chair of Trustees will then investigate and consider what action should be taken, having obtained legal advice if required.

Where there has been a breach of European Data Protection Legislation the Chair of Trustees must notify the Information Commissioner's Office without undue delay and where feasible no later than 72 hours after the relevant individual Trustee first became aware of the breach unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The Chair of Trustees should submit the report electronically to casework@ico.org.uk or on the Information Commissioner's Office [website](#), and retain a copy of the notification.

Where a breach of European Data Protection Legislation is likely to result in a high risk to the rights and freedoms of individuals, the Trustees must also write to any affected individuals to notify them of the breach without undue delay. Should the Chair of Trustees have any doubt as to whether a particular breach is likely to result in a high risk to the rights and freedoms of individuals, they should seek legal advice.

8 COMPLIANCE WITH THIS POLICY

The Trustees will review this Policy every two years unless there are circumstances that merit an earlier review. It will monitor compliance with this Policy through its Risk Register.

As part of its Trustees' training programme all individual Trustees' will be provided with data protection and security training. Refresher training will also be provided to individual Trustees as appropriate.

The Trustees are not required to have a Data Protection Officer under European Data Protection Legislation as they are not a public sector organisation, their core activities do not require the regular and systematic monitoring of data subjects on a large scale nor does their core activities require the processing of special category data and data relating to criminal convictions and offences. They have decided, therefore, not to appoint one.

Should an individual Trustee have any queries in relation to this Policy, they should contact the Chair of Trustees in the first instance.

Policy created 25 May 2018

Updated December 2018

Trustees of the UCAS Pension & Life Assurance Scheme (1993)

Fair Processing Notice

Your privacy is important to us. We will process your personal data in accordance with applicable data protection law.

The Joint data controllers in respect of the personal data you submit to us either directly or via your employer, The Universities & Colleges Admissions Service (UCAS), are the Trustees of the **UCAS Pension & Life Assurance Scheme (1993)** (the “Scheme”) and the Scheme Actuary Susanna Morran, both of whom you can contact c/o Barnett Waddingham LLP, St James’s House, St James’s Square, Cheltenham GL50 3PR. We use your personal data that is provided to us to administer and manage your pension and pay you or any person in respect of you the benefits provided by the Scheme.

We process the personal data that you provide to us for the purpose of administering and managing your pension and paying you and/or your spouse and dependants benefits and managing the Scheme as a whole. We therefore process your personal data on the legal basis that the processing is necessary for the performance of the contract of employment between you and UCAS regarding your participation in the Scheme, to comply with our legal obligations and further to our legitimate interests as trustees of the Scheme. If you do not provide us with the personal data that we specify is required for administration of the Scheme then we may not be able to administer the benefits provided by it.

We will transfer your data to UCAS and other participating employers in its group and their advisers, the Scheme's advisers, service providers and partner organisations to the extent that it is necessary for the management and administration of the benefits provided by the Scheme. We may also disclose your information to third parties in order to operate, administer and audit the Scheme responsibly, in the event that UCAS sells its business or assets (in which case we may disclose your personal data to the prospective buyer), in the event that we decide to de-risk or insure any of the benefits provided by the Scheme (in which case we may disclose your personal data to the prospective insurer) or where we are under a duty to disclose your personal data in order to comply with any legal obligation or to protect the rights, property, or safety of the Trustees, the members of the Scheme, or others. We do not use your data for marketing or transfer personal data to other organisations for the purpose of marketing their goods or services.

Your personal data may be processed outside of the European Economic Area ("EEA") where required in order for us or UCAS to provide benefits to or in respect of you. In each instance, we have ensured that the processing of your personal data outside the EEA is governed by the Standard Contractual Clauses approved by the European Commission.

We will keep your personal data stored on our systems for as long as it takes us to provide the pension and other benefits provided under the rules of the Scheme. We will retain and use your information as necessary to comply with our legal obligations, resolve disputes and enforce our rights. We review our data retention policies regularly and will retain your personal data only as long as necessary for the purpose for which we process that data.

Data Protection legislation gives you the right to access information held about you. Where we or third parties are processing your personal data on the basis that you have consented to that processing then you are entitled to withdraw your consent. If you do withdraw your consent, we may still be able to process some of the data that you have provided to us on other grounds. However, some data, for example data in relation to your health or personal life, is regarded as 'special categories of data' [We have to process that special category data to perform our obligations under employment law and the law relating to social protection. Therefore, we do not require your specific consent to process that information]

From 25 May 2018, you will be entitled to receive the personal data that you have provided to us in a structured, commonly used and machine-readable format, and to transmit that data to another data controller. You can exercise your data protection rights, including your rights to access, restrict, object to the processing of, rectify and erase your personal data by contacting Barnett Waddingham at the address above. If you are unhappy with the way in which your personal data is being processed you have a right to lodge a complaint with the Information Commissioner's Office. You can report your concerns by telephoning their helpline on 0303 123 1113 or through their website at <https://ico.org.uk/concerns>.