TRUSTEE'S DATA PROTECTION POLICY

MRC PENSION SCHEME

CONTENTS

1. INTRODUCTION

This Policy sets out the rules adopted by M.R.C. Pension Trust Limited, the sole corporate trustee of the MRC Pension Scheme (the Trustee and Scheme, respectively) in respect of data protection and the conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

The Policy, the inventory of processing activities (see below) and risk register (see **Section 2**) are reviewed by the Trustee regularly and following any material changes that may impact the processing of the personal data for which it is responsible and any material change to legislation or guidance.

The Trustee has obtained professional advice regarding the matters set out in this policy document.

Date of last review: November 2021.

BACKGROUND

The Trustee is responsible for the capture, maintenance, processing and security of all personal data held as part of the Scheme and necessary for the administration and management of the Scheme.

The Trustee's responsibilities are significant and are governed by, inter alia, Trust and Pensions Law, the Rules of the Scheme, the General Data Protection Regulation (as transposed into UK national law) (GDPR) and the Data Protection Act 2018 (Data Protection Laws). References to GDPR, the Data Protection Act 2018 and/or Data Protection Laws in this document should, where appropriate, be interpreted as including any legislation that replaces it.

The Trustee recognises that it processes data in respect of other categories of individuals, e.g. individual directors of the Trustee (the Trustee Directors). Data relating to these data subjects are also covered by this Policy.

In developing this Policy, the Trustee has considered relevant law and practice in relation to the processing of personal data in the context of pension schemes.

The objective of the Policy is to provide a framework that will assist in compliance with data protection obligations in relation to Scheme personal data, not just by the Trustee but also its delegated authorities including, where appropriate, the sponsoring employers of the Scheme.

ROLE OF THE TRUSTEE

The Trustee is a Controller in respect of the Scheme.

PURPOSES FOR WHICH DATA ARE PROCESSED

The processing for which the Trustee is responsible and the purposes for which they are generally undertaken are described in the following table.

Purposes for which personal data is processed
Occupational pension scheme administration, including payment of benefits to and in respect of pension scheme members and beneficiaries on leaving service, retirement and death; communication with members and other beneficiaries; financial reporting; and investment of assets
Occupational pension scheme payroll, including payment of pensions to members and beneficiaries and accounting to HMRC for tax on pensions

In more detail, processing activities in respect of members, beneficiaries and other data subjects include but are not restricted to –

- Issuing communications and information
- Responding to queries and disputes
- Calculation and payment of benefits (including pensions, lump sums and transfer values)
- Establishing eligibility for benefits
- Calculation and reconciliation of contributions
- Payment of tax charges and monitoring whether pension tax allowances are exceeded
- Reporting to HMRC
- Ensuring compliance with contracting-out requirements
- Preparation of Scheme financial statements and other returns
- Actuarial valuations, updates and calculations
- Investment of Scheme assets
- Obtaining or preparing quotes for annuities or other insurance contracts
- Purchasing annuities or other insurance contracts
- Managing Scheme risk
- Exercising Trustee's powers and discretions
- Carrying out any other activity which is incidental to the performance of Trustee's duties in relation to the Scheme.

CATEGORIES OF PERSONAL DATA PROCESSED

The categories of personal data that the Trustee processes are described in the following table.

Categories of personal data processed
Personal attributes : Name; address, Age or date of birth; identifier(s); marital information (including divorce); gender; employment history; remuneration information; National Insurance Number; PAYE information; bank account details
Special Categories of Data : Health information; medical diagnosis information; race or ethnic origin; sexual orientation; religious / philosophical / political beliefs; membership of trade union
'Other' Scheme membership information, including details of pension contributions and benefits; nomination forms; and adviser / service provider details

DATA SUBJECTS

The Data Subjects to which this Policy applies include all of the Scheme beneficiaries and other individuals in the table below.

Categories of data subjects
Members who have left the Scheme
A pensioner who is drawing a pension or other form of benefit from the Scheme
A contingent beneficiary of any other above membership categories e.g. a spouse or child dependant
Anyone acting on behalf of a deceased member of the Scheme e.g. a family member or friend of the deceased
A legal representative of a member of the Scheme
A Financial Adviser formally appointed by a member of the Scheme

TRUSTEE DIRECTORS' PERSONAL DATA

The Trustee also processes data in respect of individual Trustee Directors. The categories of data processed for individual Trustee Directors are name, phone number, address and e-mail address. Processing activities include, but are not restricted to, issuing communications, information and meeting packs; preparation of Scheme rules and amending deeds; payment of expenses; reporting to HMRC, the Pensions Regulator and other bodies; and preparation of Scheme report and accounts.

LEGAL BASIS OR BASES FOR PROCESSING PERSONAL DATA

The Trustee is responsible for ensuring that it has an appropriate legal basis for the processing of Scheme personal data as identified in the Data Protection Laws. The Trustee's legal basis for processing personal data may vary according to data subject, category of data held and / or purposes for which it is used. In some circumstances more than one legal basis for processing personal data may apply to a particular category of processing.

The processing described above (other than the processing of special category data) is generally necessary for the legitimate interests of administering the Scheme and related purposes set out above. The Trustee has carried out an assessment and does not consider that this processing will prejudice the interests, rights or freedoms of the data subjects.

The Trustee also processes personal data to fulfil itsr legal obligations under the Pensions Acts and the Scheme's governing documentation.

Explicit consent is obtained for the processing of special category data. Consent may also be used as a basis for processing personal data in other circumstances.

The specific basis or bases for processing the different categories of personal data processed by the Trustee is set out in the table below.

Categories of personal data processed	Legal basis or bases
Personal attributes: Name; address, Age or date of birth; identifier(s); marital information (including divorce); gender; employment history; remuneration information; National Insurance Number; PAYE information; bank account details	Legitimate Interest and Legal Obligation
Special Categories of Data: Health information; medical diagnosis information; race or ethnic origin; sexual orientation; religious / philosophical / political beliefs; membership of trade union	Consent, Legitimate Interest and Legal Obligation
'Other' Scheme membership information, including details of pension contributions and benefits; nomination forms; and adviser / service provider details	Legitimate Interest and Legal Obligation

DATA PROTECTION PRINCIPLES

The Trustee recognises that, in its role as Controller, it is directly responsible for compliance with all aspects of the Data Protection Laws and for demonstrating compliance in respect of the Scheme. It recognises that if this is not achieved then a liability to pay damages may arise, and the Trustee could be subject to fines or other penalties and / or sanctions.

The Trustee is responsible for and must demonstrate compliance with the principles of the Data Protection Laws. The principles are:

- **Lawfulness, fairness and transparency:** data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation:** data must be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes.

- **Data minimisation:** data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** data must be accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that inaccurate personal data are erased or rectified without delay.
- **Storage limitation:** data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.
- **Integrity and confidentiality:** processing must ensure appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. TRUSTEE'S POLICY

Issue	Policy
Data strategy approach	The Trustee has taken and will continue to take professional advice on the application of the Data Protection Laws to the Scheme. The Trustee has obtained input from the processors it has contracted with to provide services to the Scheme, and provides instruction to those processors in respect of the Trustee's approach to the Data Protections Laws. The Trustee has added data protection and security to its 'Trustee Knowledge and Understanding' (TKU) requirements for Trustee Director training. The Trustee has put in place protocols in relation to conduct and proceedings (**Section 6**).
Data Protection Officer	The Trustee has taken professional advice and determined that it is not required to appoint a Data Protection Officer.
Data Protection Impact Assessments	The Trustee is aware of the requirements for Data Protection Impact Assessments (DPIAs) and the forms of processing which may trigger DPIAs. DPIAs will be carried out where required by the Data Protection Laws.
Records of processing activities	The Trustee maintains a record of processing activities in line with the requirements of the Data Protection Laws.
Privacy notices	The Trustee is responsible for the content and issue of privacy notices in line with the Data Protection Laws.
Consent	The Trustee will obtain, record and monitor the explicit consent from data subjects to process any special category personal data. For data other than special category data, the legal basis / legal bases for processing is / are described in Section 1.
Data Subject Rights	The Trustee recognises the rights of the data subject as set out in the Data Protection Laws, including – • its right of access to information • its right to have information corrected or updated • its right to be forgotten • its right to restrict processing. Trustee Director training on data protection and security includes data subject rights. Data subjects wishing to exercise their rights are required to write to the Trustee (email or paper) setting out their request.

Issue	Policy
	The Trustee will review the request within 5 working days to establish whether the request is valid. The Trustee will seek professional advice, if necessary. On completion of the review, the Trustee will contact all relevant processors that need to support the request. **Subject access requests must be responded to within a month.** The Trustee is aware that, in certain circumstances, legislation allows personal data to be disclosed without the consent of the data subject. The Trustee acknowledges that, in certain circumstances, personal data will be disclosed without such consent or even knowledge of the data subject. The Trustee will ensure that its processors are obliged to comply with the rights of data subjects as set out in the Data Protection Laws. The Trustee will assess the impact of new rights on the Scheme and up-date these policies accordingly.
Privacy by Design and Default	Compliance with data protection regulation is proactively taken into account when designing or reviewing processes and applications that affect personal data. The Trustee will handle personal data and needs to take into account privacy by design and default. The Trustee will discuss the introduction of additional audit tests as required to assess compliance with the Data Protection Laws.
Supply chain management	See **Section 3**.
Personal data security	The Trustee will implement appropriate technical and organisational measures in respect of personal data security. These will include – • processes for regularly testing, assessing and evaluating the effectiveness of security measures • measures to guard against the risks of accidental or unlawful destruction of personal data, data loss or alteration and unauthorised disclosure of, or access to, personal data, and obligations to notify the Trustee promptly of any such events occurring • measures preventing the processing of personal data other than on the explicit instructions of the Trustee. See also **Section 6**.
Transferring personal data outside of the United Kingdom and the EEA	The Trustee permits its processors to transfer personal data to locations outside of the United Kingdom and the EEA, subject to its consent in writing. The Trustee will require any processor who transfers personal data to a location outside of the UK and/or EEA to put in place appropriate safeguards before doing so, such as: • use of model clause agreements that have been approved by relevant regulators; • not transferring personal data outside of the UK and/or the EEA until appropriate checks have been made; and/or • ensuring administrators have processes in place to consider data protection whenever a Scheme member or beneficiary requests an overseas transfer.
Data protection and security compliance monitoring	Risks in relation to data protection and the Data Protection Laws are recorded and reviewed on the Trustee's risk register.

Issue	Policy
	The Trustee has included data protection and security within its internal audit scope to test compliance, particularly in relation to regular penetration testing and compliance by the third party administrator. The Trustee includes data protection as a standing agenda item under governance at its meetings, including the review of management information regarding data subject rights, breaches and developments in legislation, Regulator guidance and best practice. The Trustee seeks governance advice and practical assistance in reviewing risk and compliance.

3. PROCESSORS / SERVICE PROVIDERS AND SHARING DATA WITH OTHER THIRD PARTIES

This section sets out the Trustee's policy regarding the use of processors and other service providers as well as its policy regarding the sharing of personal data with other third parties.

APPOINTING A NEW PROCESSOR AND/OR OTHER SERVICE PROVIDER

Those service providers of the Trustee which process personal data in the course of providing services to the Trustee or who process personal data as data processors for and / or on behalf of the Trustee are included under this Section 3.

As part of the appointment of individuals and organisations, the Trustee will require them to provide a written statement of compliance with the Data Protection Laws and the Trustee's specific requirements for the Scheme. In particular, relevant service providers will be required to demonstrate how they keep data secure and how they test their security arrangements.

Service providers must enter into a contract for services with the Trustee, which will include the specific requirements of the Data Protection Laws.

In addition, each contract with a processor will comply with Section 59 of the Data Protection Act 2018 and include, inter alia, the following provisions.

- Processors must:
  - process personal data only on documented instructions from the controller;
  - ensure that persons authorised to process the personal data have committed themselves to confidentiality;
  - take all measures required by the Data Protection Laws regarding the security of processing personal data;
  - assist the controller's obligation to respond to requests for exercising the data subject's rights and managing personal data breaches.
- Further, each contract between the Trustee and its processors must set out:
  - the subject-matter and duration of the processing
  - the nature and purpose of the processing
  - the type of personal data
  - the categories of data subjects and
  - the obligations and rights of the controller.

PROCESSORS / SERVICE PROVIDERS

The organisations and individuals which process personal data in the course of providing services to the Trustee or who process personal data as data processors for and / or on behalf of the Trustee are listed below.

Position	Name	Capacity
Current Scheme Actuary	Sue Vivian, Government Actuary's Department	Controller
Scheme Administrator	Mercer	Processor
Previous Scheme Administrator	Medical Research Council	Processor
Scheme Auditors	KPMG LLP	Processor
Internal auditor	BDO LLP	Processor
Legal Adviser	DLA Piper UK LLP	Controller
Investment Managers		Processor
Investment Consultant	Redington Ltd	Processor
Sponsoring employer	United Kingdom Research and Innovation	Processor
Printer / Communications provider		Processor
AVC provider	Utmost Life Standard Life	Processor
Member tracing provider		Sub-processor of Mercer
Independent medical adviser	RPS Business Healthcare	Processor

TRUSTEE'S CRITERIA FOR PROCESSORS / SERVICE PROVIDERS

Requirements	Comments
General	The Trustee requires confirmation that relevant staff of UKRI (including Trustee Directors who are employed by UKRI) have been trained in the requirements and behaviours necessary to be compliant with the Data Protection Laws. The Trustee requires processors to advise it of all changes in approach which may affect compliance with the Data Protection Laws so that the Trustee can, where necessary, provide instruction.
Records of processing activities	The Trustee requires confirmation that a record of processing activities is maintained in line with the requirements of the Data Protection Laws.
Privacy by Design & Default	The Trustee requires regular confirmation that data protection regulation is proactively taken into account when designing or reviewing processes and applications that affect personal data. The Trustee will discuss and agree the introduction of additional audit tests as required to assess compliance with the Data Protection Laws.
Data Protection Impact Assessment (DPIA)	Where the requirement for a DPIA applies, confirmation will be provided that one has been undertaken.
Data Protection Officer	Where the requirement for a data protection officer applies, their name and contact details will be provided.

SHARING DATA WITH THIRD PARTIES

The Trustee will only provide personal data to third parties who request access to Scheme personal data where it has determined that the party in question it is entitled to do so under the Data Protection Laws and in a manner compliant with the Data Protection Laws. In addition to those processors/service providers described above, parties that personal data may be provided to include, but are not limited to, the following:

- Her Majesty's Revenue and Customs (HMRC)
- The Pensions Regulator
- The Pensions Ombudsman
- Department for Work and Pensions
- The Pensions Advisory Service
- The Courts
- The Police

The Trustee may share data with UKRI or another employer provided there is a legal basis or bases for sharing it, and the Trustee is satisfied that it is appropriate to do so.

The Trustee will always document the legal basis or bases relied upon whenever data is shared with a third party, including UKRI or another employer.

For subject access requests, see **Section 2**.

4. DATA RETENTION

Pensions are long-term benefits in that members build up their benefits over very long periods and can be drawing benefits for twenty years or more.

Additionally, it is not unusual for disputes to occur which require interrogation of Scheme data going back decades.

The Scheme's data are held in a number of different ways by the Trustee and different delegated authorities / service providers, and for different periods and reasons.

However, Scheme data will be held only for so long as is necessary for the proper and compliant governance and administration of the Scheme. Where data is no longer required, it will be destroyed in a manner that ensures it is put permanently beyond use; e.g.

- Where data is held in a paper format, destruction means that the data will be shredded.
- Where data is held by third parties, the Trustee will rely on confirmation from them that data has been destroyed.

The maximum periods that the Trustee will normally hold / process personal data are as follows –

- For so long as any benefit is secured or payable under the Scheme to or in respect of a member or beneficiary, the Trustee will retain so much of their personal data as is necessary to ensure that benefits can be paid correctly.
- Where benefits cease to be payable or secured under the Scheme, e.g. in the case of transfer-out, a pension benefit buy-out or benefits being otherwise discharged, the Trustee will continue to hold such personal data as the Trustee considers is necessary to fulfil the purposes of the Scheme as set out in Section 1 and / or deal with any complaint or dispute in relation to any benefit entitlement.
- The Trustee will never process or hold on to data for longer than the life of the Scheme plus 15 years.

The Trustee will obtain a copy of and review the data retention / deletion policy for each data processor / service provider that it has contracted with in accordance with Section 3 to ensure compliance with the Data Protection Laws.

The Trustee has considered, agreed with the relevant processor(s) and documented how it will validate Scheme data relating to current members (active, deferred and pensioner). The Trustee has also considered, agreed with the relevant processor(s) and documented how best to audit historic records before making a decision on what to retain and what to destroy.

Where the Trustee holds data in relation to matters other than the payment of benefits under the Scheme (eg the personal details of the Trustee Directors), such data will be held for such periods as are considered by the Trustee to be reasonable, and appropriate.

5. PERSONAL DATA BREACH

INTRODUCTION AND SCOPE

The Trustee is committed to handling personal data securely and properly. Security incidents may pose significant risks, unless handled appropriately. Security incidents should therefore involve timely reporting, reactive, preventative and risk mitigation activities and be handled at all times in accordance with this Policy.

The purpose of this section is to provide clear guidelines to the Trustee and the Trustee Directors on how to identify and deal with a security incident involving a personal data breach, which may constitute a breach of data protection laws and/or require notification to the Information Commissioner's Office and (where applicable) affected data subjects.

DEFINITION OF A PERSONAL DATA BREACH

Personal data breaches should be distinguished from other security incidents; it is possible for Scheme personal data to be subject to a security incident which is not also personal data breach, in which case the regulatory notification requirements which may apply in relation to a personal data breach will not be relevant.

A "**security incident**" is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information, interference with IT systems, operations, or an event that can result in or present an imminent threat of a violation of standard security practices, or IT security policies. For example, a security incident may include:

- unauthorised access of IT systems;
- unauthorised system changes such as suspicious account deletions or unauthorised server reboots;
- denial of service attacks;
- use of malicious codes such as a worms, malware or viruses;
- inappropriate use of information technology assets;
- social engineering attempts;
- unlawful activity including gross misconduct; or
- breach of server or network attached devices.

A "**personal data breach**" means a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personal data breaches can arise from a range of circumstances, from deliberate third party attacks on IT infrastructure hosting Scheme personal data designed to harvest personal data for criminal purposes, to the accidental loss of storage devices (i.e. mobile phones, laptops, USB devices) by a Trustee Director or processor acting on behalf of the Scheme.

DETECTING AND RESPONDING TO A PERSONAL DATA BREACH

Personal data breaches should be dealt with according to a four stage approach involving (1) **identification**; (2) **assessment**; (3) **response handling**; and (4) **review**. Each stage is explained in more detail below.

IDENTIFICATION OF A PERSONAL DATA BREACH

Personal data breaches are likely to be detected through internal reporting and third party processor/external notifications.

All processors are required by contract to report any personal data breach to the chair of the Trustee Boards (the Chair) (or nominated deputy if he/she is not available for any reason) within 24 hours of that breach being identified. Where a notification is provided to any other Trustee Director, it is important that this is escalated to the Chair immediately.

Any Trustee Director that is made aware of a personal data breach (either where the Trustee Director has themselves identified the breach or has been made aware by a third party processor) must inform the Chair immediately (and in any event within 24 hours of that breach being identified). The Chair will then inform all other Trustee Directors.

The Trustee Directors receive training on how to identify a personal data breach.

The Trustee has implemented measures to detect potential personal data breaches. These include:

- Requiring Processors to inform the Trustee of a data breach as soon as practicable/ possible after they have become aware of it.
- Taking into account guidance on data breach handling issued by the Information Commissioner's Office and the European Data Protection Board (the EU data protection advisory body).

ASSESSMENT AND PERSONAL DATA BREACH MANAGEMENT

The Chair, the Director of MRC Pensions / Scheme Secretary and at least one other Trustee Director (or two other Trustee Directors, if the Chair is unavailable) (the Response Team) must review the breach and, taking into account any guidance from the Information Commissioner's Office and the European Data Protection Board (whose guidance is still endorsed by the Information Commissioner's Office notwithstanding the UK's departure from the European Union) on data breach handling, determine whether the breach is:

- Unlikely to result in a risk to the rights and freedoms of natural persons. Examples include where the Trustee has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.
- Likely to result in a risk to the rights and freedoms of natural persons.
- Likely to result in a high risk to the rights and freedoms of natural persons.

If the Chair is unavailable, either by his own determination or if unresponsive to a relevant email with two hours of issue, then Mr Dunlop (or such other Trustee Director appointed by UKRI and notified to the Scheme Secretary from time to time) shall replace the Chair on the Response Team for the purposes of the relevant breach.

If the Director of MRC Pensions / Scheme Secretary is unavailable, as determined by the Chair, then another Trustee Director shall replace the Director of MRC Pensions / Scheme Secretary for the purposes of the relevant breach.

The outcome of this review must be documented.

The Chair and/or the Director of MRC Pensions / Scheme Secretary:

- may call an exceptional Trustee's meeting to discuss the breach;
- may convene an initial meeting of the Response Team to agree the resolution strategy;
- should consider the appointment of legal advisers taking into account the severity of the breach; and
- will also inform the sponsoring employer, via Hugh Dunlop at United Kingdom Research and Innovation, and the Client Relationship Manager, at Mercer, within 24 hours of being notified of a breach (to the extent that the breach was not initially notified by Mercer to the Trustee).

RESPONSE HANDLING

The precise action to the taken by the Response Team, led by the Chair (or the Director of MRC Pensions / Scheme Secretary, if the Chair is unavailable), will depend on the nature of the personal data breach, however it is likely to include:

- **investigation:** to understand the nature of the incident, the impact on the Scheme (in terms of legal liability, reputational damage, financial impact, organisational impact and other risk factors) and help establish the underlying cause and establish impacted individuals;
- **containment:** of the breach to prevent any further data loss or security compromises, which may involve, for example, taking systems offline;
- **restoration:** of any systems impacted by the breach as soon as possible once the breach has been contained, this may include recovering data from suitable backup systems;
- **intervention and improvement:** to existing processes to prevent recurrence of the incident, this may be supported by targeted security awareness training or legal action; and
- **engagement with stakeholders:** it is important to effectively engage with those directly affected by, or who may have a wider interest in management of, the breach. This may include Scheme members, the media, and appropriate regulators (in particular the ICO) or law enforcement.

The Response Team should always consider whether guidance from an external legal advisor should be sought before any information relating to the incident is disclosed. This is to ensure any disclosures are accurate and do not expose the Scheme to undue risk. Guidance should also be sought from external legal advisors to determine whether and how to report a personal data breaches to regulators.

As referred to above, the decision as to whether or not a personal data breach is required to be notified either to the ICO and/or impacted individuals will be determined by the severity assessment carried out by the Response Team referred to above, and outlined in more detail below:

Likely to result in a risk to the rights and freedoms of natural persons

If the breach is likely to result in a risk to the rights and freedoms of natural persons then the Trustee must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO.

Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The notification to the ICO shall include as a minimum:

- Description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- The name and contact details of the contact point where more information can be obtained;
- Description of the likely consequences of the personal data breach;
- Description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Likely to result in a high risk to the rights and freedoms of natural persons

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least:

- The name and contact details of the data protection officer or other contact point where more information can be obtained;
- Description of the likely consequences of the personal data breach;
- Description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The communication to the data subject shall not be required if any of the following conditions are met:

- The Trustee has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

REVIEW

DOCUMENTATION AND REMEDIAL ACTION

The Trustee shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken (both in respect of the breach and to reduce the risk of a further occurrence). This applies to all personal data breaches, whether or not any regulatory notification was required in connection with the breach.

All processors are required by contract to support the root cause analysis and remedial action where appropriate.

The Response Team will hold a post-incident review meeting to cover the following issues:

- did the detection and response procedures work as intended;
- if not, what areas need to be amended;
- what changes could be made to procedures to improve the Trustee's ability to detect and deal with a similar incident;
- what aspects worked well and what additional tools would be useful for the future;
- was the level of the Trustee's response appropriate; and
- could any lessons be learnt from the incident. In particular, should any identified improvements be implemented into this policy for application for subsequent incident response.

6. CONDUCT AND PROCEEDINGS

INTRODUCTION

The Trustee recognises that as Controller under the Data Protection Laws, it must make sure that it has appropriate systems and policies in place in respect of the Trustee Directors' own activity to adequately protect member data and Scheme information and data (including information provided by UKRI and any other Scheme employer).

All Trustee Directors should follow the General Principles below. In addition, specific arrangements should be followed for certain types of Trustee Director.

GENERAL PRINCIPLES

These arrangements apply to all Trustee Directors, in so far as they apply individually to them and support the Trustee otherwise in achieving these General Principals:

- Scheme documents/Portal
  - Key Scheme documents are to be stored on a secure website (currently Diligent Boards) (the Portal).
  - Access to the Portal will be limited to the Trustee Directors, the Scheme Secretary and specified individuals within advisers of the Trustee, as permitted by the Chair and Scheme Secretary, where access is necessary for required advice and/or support to the Trustee.
  - A list of those given access to the Portal (and which areas on the Portal) will be kept by the Scheme Secretary from time to time.
- Trustee meeting papers
  - The Trustee aims to use the Portal, as far as is reasonably practicable, to distribute and provide access to all papers for Trustee meetings.
  - In so far as any papers need to be circulated, otherwise than through the Portal:
    - they shall be circulated by email;
    - any emails containing personal data/information shall be password protected;
    - any emails are also to be held/saved securely (i.e. with firewall, password protection, encryption in place).
  - Hard copy meeting packs issued to the Trustee Directors:
    - shall be by exception, and only with the prior consent of the Chair;
    - shall be kept physically safe; and
    - shall be securely destroyed after no more than 1 month following the meeting date, and confirmation immediately provided to the Scheme Secretary by email that this has been completed;

- Keep any confidential information secure
  - Any papers, files, laptops, mobile devices, etc containing Scheme information or personal data are kept physically safe.
  - Make sure nobody can see the screen or any papers, if working in a public place or otherwise.
  - Shred confidential Scheme information and personal data. Dispose of equipment holding Scheme information or personal data, securely.
  - Make sure devices are locked using a form of secured access (for example, a password, fingerprint or facial recognition or equivalent means of secured access) when not in use. Be mindful of the need for a secure password and take care to avoid taking action that could help hackers to discover passwords.
  - Ensure that anti-virus and firewall software is up to date, and that all updates for applications and operating systems are implemented.
  - Take care that appropriate security procedures are followed in relation to using external devices on Scheme operating systems, for example confirming the security of (and if necessary restricting the use of) USBs, external hard drives and CD-Roms etc.
- Transfer of data/information
  - Do not provide Scheme information or personal data to anyone, either online or over the phone [without seeking appropriate assurances that the information should be shared with them].
  - If transferring personal data, ensure it is appropriately protected (for example with a password or by sharing data via Diligent Boards[1]).
  - Do not share personal data unless it is necessary. Consider and use anonymised information if possible.
- Storage of data
  - Do not keep original documents at home or in ad hoc locations at a workplace.
  - No confidential information or member data should be discussed, shared or made accessible to any person other than a Trustee Director, Scheme Secretary or adviser to the Trustee.
- Physically safe

  Where the term "physically safe" is used in this Section 6, it shall mean that:
  - Trustee Directors have the personal obligation to ensure the standard of being physically safe is met, taking into account all relevant circumstances at the relevant time;
  - as a minimum and applicable in all cases, it shall require Trustee Directors to:
    - ensure that at all times Trustee Directors are present with and aware of the safety of the relevant items;
    - if not present with the relevant items, steps are taken to ensure that the relevant items:
      - cannot be printed, copied, sent, or viewed/read by any person other than another Trustee Director in the performance of their role;
      - such steps may, where appropriate, include:
        - a locked cabinet, where nobody else has access to the key;
        - a locked room, where nobody else has access to the key, other than a formal security function; or
        - locking in the boot of a car for a short period, no more than 15 minutes.

[1] The Trustee and the Scheme Secretary will need to monitor whether the Trustee Directors currently use Diligent Boards in this manner and whether they will continue to do so.

TRUSTEE DIRECTORS WHO ARE EMPLOYEES OF UKRI

Any Trustee Director who is an employee of UKRI:

- shall follow the appropriate policies for cyber and data security as required by UKRI;
- shall use UKRI email addresses and shall ensure that electronic Scheme information is stored on the personal folder within the UKRI network;
- should avoid having paper records, if at all reasonably possible, but where possessed stored in locked cabinets whilst at work premises;
- as far as reasonably possible, ensure that Scheme information on emails and otherwise is not accessible by anyone else; and
- ensure that Information will be backed up in accordance with normal UKRI policies and procedures.

OTHER TRUSTEE DIRECTORS

- It is recognised that some Trustee Directors may not have access to the infrastructure available to UKRI. However, they should consider their own arrangements carefully and seek advice from the Chair and/or the Scheme Secretary, if they have any concerns about security.
- They should ensure that Scheme information and data cannot be accessed by other household members (for example the use of shared email addresses is not acceptable and data saved on a PC with shared access must be password protected), or others.
- Paper records should be avoided if at all reasonably possible, but where possessed stored in locked cabinets.
- Where a Trustee Director is employed and the security/privacy arrangements are appropriate, it may be that a Trustee Director uses their email address for their employment. Again, a Trustee Director should consider the arrangements relevant to them and seek advice from the Chair and/or the Scheme Secretary, if they have any concerns about security and/or confidentiality.

CEASING TO BE A TRUSTEE DIRECTOR

On ceasing to be a Trustee Director, all personal data, and all Scheme information, data and access details (including any information or data on UKRI or other Scheme employers) will be safely and securely returned to the current Trustee or destroyed within 3 months. This includes electronic and hard copy data (if any). Confirmation of compliance with this requirement must be provided to the Scheme Secretary.

DATA MINIMISATION

Each Trustee Director will consider the personal data held by them periodically and delete any documents that are duplicated elsewhere and no longer required by that Trustee Director.

It is recognised that any professional trustee may not delete duplicate information as this could be required in future to address queries or complaints it receives.

INCIDENT RESPONSE

If a Trustee Director becomes aware of a security breach, he or she must follow the arrangements set out in Section 5 (Personal Data Breach).

MONITORING AND REVIEW

This Section 6 and adherence to it will be monitored regularly at Trustee meetings.

The Section itself will be reviewed periodically and (1) at least every three years[2] and (2) promptly following any material changes in Data Protection Laws or developments in other laws relating to information security.

Data security is included in the trustee knowledge and understanding ('TKU') programme.

Communication with and reassurance given to members about personal data is via a regular newsletter.

[2] The Trustee may wish to review the policy more frequently following the introduction of the Data Protection Laws, in order to ensure that any new guidance or information from the ICO can be incorporated into the drafting of this policy if required. We haven't 'hard coded' this in, and the Trustee is free to review the policy more frequently than is set out in it (but not less frequently).

APPENDIX - GLOSSARY OF IMPORTANT TERMS

Personal data	Information relating to an identifiable person. Note that a person may be identifiable in many different ways and that the definition extends to data that could be linked to a specific individual by use of other data in the possession or control of the Trustee or its processors and also data that they may be able to obtain from public sources.
Special category [formerly sensitive] data	Reveals racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; data concerning health or sex life and sexual orientation; genetic or biometric data.
Processing	Operations performed on personal data. This is very wide ranging as it captures anything that can be done with data and includes simply storing it, accessing it and deleting it.
Controller	Body that determines the purpose and means of the processing of the personal data. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.
Processor	Body that carries out processing on behalf of the controller.
Data Subject	A natural person whose personal data are processed by a Controller or Processor.
Data Protection Impact Assessment	Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Privacy by Design and Default	This concept can be best described, in a data protection context, as ensuring that compliance with data protection regulation is not an after-thought but proactively taken into account when designing or reviewing processes and applications that affect personal data.

CONTACT

Trustees:	**M.R.C. Pension Trust Limited**	
	Registered Address:	**David Phillips Building** **Polaris House** **North Star Avenue** **Swindon, SN2 1FL**
	Correspondence Address:	**58 Victoria Embankment, London EC4Y 0DS Street**
Pensions Administrators:	**Mercer**	
	Correspondence Address:	**Leatherhead House** **Station Road** **Leatherhead, KT22 7ET**
Member website:	**www.mrcps.co.uk**	