Appendix I

Processing activities for which LawDeb Pension Trustees are responsible

1. **The data subjects for a pension scheme are:**
    - Active members
    - Deferred members
    - Pensioners (including those in receipt of a dependant's or a spouse's pension)
    - Prospective members who will or may receive benefits from the scheme (for example on the death or divorce of a member)
    - Former members (for example members who have died or transferred out of the scheme)
    - Ex-spouses of members (for example following a pension sharing order)
    - Persons who claim to be members.

2. **Third parties with whom data may be shared:**
    - Trustees' professional advisers (for example legal advisers, auditors, actuaries, communication consultants, investment consultants)
    - Service providers (for example administrators, payroll providers, printing agencies, banks and tracing agencies)
    - Participating employers
    - Insurance providers
    - Regulatory authorities (for example the Pensions Regulator and HM Revenue & Customs)

3. Categories of personal information that may be held

- Employment and pension scheme membership data including dates of joining and leaving employment, periods of pensionable service, earnings and details of other benefits.
- Personal data including name, date of birth, sex, contact details (eg home address, telephone numbers and e-mail address), identifiers such as National Insurance number.
- Pension contribution and benefit data, including compulsory and voluntary contributions, actual or potential defined benefits, defined contribution account information (eg investment allocation and account balance).
- Other financial data such as National Insurance contributions, bank sort code and account number, tax code, Lifetime Allowance and other protections.
- Family data and data regarding personal circumstances including current marriage or civil partnership, any previous relationships and dependants, death benefit expression of wishes and distribution information.
- Identification documents including birth, marriage, civil partnership and death certificates, passport identity pages, decree absolute, pension sharing and earmarking orders, Wills.
- Personal health data in connection with eligibility for ill-health and death benefits and payment of ill-health benefits.

4. Purposes of processing the data

- To confirm a member's identity and establish the eligibility for benefits.
- To pay pension benefits and deal with any questions about these.
- To pay tax charges, monitor whether allowances are exceeded and report to HM Revenue & Customs.
- To meet the compliance requirements with regulatory legal obligations, such as reporting to relevant authorities and government bodies.
- For risk management purposes, including the insurance or management of longevity risks and obtaining quotations for annuities or other insurance products.
- To communicate with pension scheme members about their benefits and the pension scheme in general.
- To trace members and other beneficiaries.

Appendix II *Extract from LawDeb Pension Trustees AAF02/07 Assurance Report for the year ending 31 March 2017*

Control objective and control procedure	CCW testing of control procedures
Information technology	
Computerised information systems have restricted physical and logical access including appropriate measures to counter the threat from malicious electronic attack (e.g., firewalls, anti-virus etc).	
Law Deb's office is in a building which is managed and secured by a reputable specialist company and only employees and pre-authorised guests are allowed to enter the premises. The security guards request all building occupants and visitors to display their photo identity cards or visitors to display their photo identity cards or visitors' passes at all times. The LawDeb floor has security card controlled access and only those with recognised cards or accompanied guests are permitted on the floor.	Through observation we verified that only employees and pre-authorised guests are allowed to enter the premises and access to the floor is card controlled. **No exceptions were identified.**
The computer systems are housed within a secure server room accessible only to authorised members of the Law Debenture Group's in-house IT staff.	Through observation and discussion we confirmed that the computer systems are housed within a secure server room accessible only the authorised staff. **No exceptions were identified.**
Additional equipment is housed at the Disaster Recovery and Business Continuity partner site and replicated in real time. Access to these premises is limited to authorised IT staff.	We obtained and inspected the contract with the Disaster Recovery and Business Continuity partner and through enquiry we verified that access to the premises is limited to authorised IT staff. **No exceptions were identified.**
Each Team member has log-in credentials including individually set passwords (meeting specified security criteria) which must be changed every 90 days. This is in accordance with IT policies contained in the Staff Handbook and Information Security Policy. All Law Debenture Group employees have to read and sign both of these documents before they are given computer access. Any amendments or updates are announced through corporate email.	Through observation we verified that access to the system is password protected. Through observation we verified that staff need to change passwords every 90 days and have agreed this statement to the Staff Handbook and Information Security policy. **No exceptions were identified.**

All LawDeb internet access is protected by appropriate firewalls and web/email filtering with a view to ensuring that no sites are accessed which could carry "malware" and incoming e-mail material is scanned against hostile material.	Through observation we verified that firewalls and web/email filters are installed across the whole network. **No exceptions were identified.**
All hosts on the Law Debenture Group's corporate LAN are protected by anti-virus solutions which are regularly patched. A central server pools the updates which are tricked through the hosts during their idle time.	Through observation we verified that anti-virus solutions are installed, and regularly updated, across the whole corporate LAN. **No exceptions were identified.**
All web access is logged against each individual's active directory account. Users are given access to virtual desktops through thin client terminals. This enhances physical security as data never leaves the dedicated server room.	Through observation we confirmed that web access is logged against each individuals accounts and that users are given access to virtual desktops through thin client terminals. **No exceptions were identified.**
Remote access is protected by two factor authentication and limited to an individual's virtual desktop. Again, all access is logged in real time and reports of successful and unsuccessful attempts stored securely and analysed regularly.	Through observation we confirmed that remote access is protected and limited to an individual's virtual desktop. **No exceptions were identified.**
Penetration testing is also performed annually by a reputable external agency which reports on potential vulnerabilities that are dealt with systematically and in accordance with best practice. This exercise is done under the terms of a strict confidentiality agreement and with detailed predetermined scopes.	We obtained and inspected the contract with the external agency and confidentiality agreement and confirmed that the penetration testing was performed during the year, as evidence of the state process being followed. **No exceptions were identified.**

Control objective and control procedure	**CCW testing of control procedures**
Maintenance and development systems, applications and software is authorised, tested, approved and implemented.	
All of the Law Debenture Group's systems are controlled and maintained by the in-house IT team. Development is performed in a	Through observation we confirmed that development is performed in a development environment and tests in a test environment and that a

development environment and tests in a test environment. A rigorous change control process if followed and only when it has been completed and documented is ti implemented in a live production environment.	rigorous change control process is followed and only when it has been completed and documented is it implemented in a live environment. **No exceptions were identified.**
As Law Debenture Group systems run on a virtual platform the three environments are exact replicas of one another. This provides an absolute separation so that maintenance and development testing is performed without the risk of affecting live production systems.	
All user change requests are logged through an ITIL complaint help desk tool which tracks activities within the IT department. Each change request is assigned a unique reference number and a brief business justification, and all relevant technical details are recorded. Only approved change requests are implemented. Should it be necessary, a change can also be reversed by restoring the prior settings. This mechanism is defined in the change management process document.	Through observation we confirmed that change requests are logged, assigned a unique reference number and only approved change requests are implemented. We obtained the change management process document. **No exceptions were identified.**

Control objective and control procedure	CCW testing of control procedures
Data and systems are backed up regularly and business and information recovery plans are documents, approved and maintained.	
Law Debenture Group's IT systems employ redundant pairs of servers in order to provide seamless service and high availability. Secondary servers are located at a dedicated disaster recovery site and replicated using a block level method. The system is managed by Vmware Site Recovery Manager Software. The IT department has its own documented business continuity procedures.	Through discussion and observation we confirmed that a redundant pairs of servers is employed and verified that daily back ups to disk are taken and recovery of data can be made. We obtained a copy of the business continuity plan to confirm in place. **No exceptions were identified.**
In addition to this built in "redundancy", there is a daily backup to disk which is carried out overnight, allowing for quick single item recovery.	
Periodic backup and restore tests are performed which consist of random items being selected to be restored. The results of the tests are recorded in reports which are stored.	We obtained and inspected the annual backup and restore test reports performed either side of the year under review to ensure back up data can be recovered. **No exceptions were identified.**