your pension our world

London Pensions Fund Authority

Information Security Policy

June 2022

London Pensions Fund Authority Information Security Policy

1. Introduction

London Pensions Fund Authority (LPFA) is committed to preserving the confidentiality, integrity and availability of all its physical and electronic information assets held in order to meet its regulatory responsibilities, maintain security, and minimise both business and reputational risks.

LPFA will adhere to the highest standards of document and information management security. LPFA treats seriously its obligations on confidentiality and data security, while maintaining adherence to the Data Protection Act 2018 (DPA 2018) and the United Kingdom General Data Protection Regulation (UK GDPR) and all other relevant regulation and legislation.

The purpose of this policy is to:

- protect against potential breaches of confidentiality and failures of integrity, or availability of information held
- ensure that the information assets and IT infrastructure are protected against damage, loss or misuse
- support the LPFA Data protection policy (see the LPFA Data Protection Policy) in ensuring all staff are aware of and comply with UK law and LPFA's own procedures applying to the processing of data
- increase awareness and understanding of LPFA's information security requirements and the responsibility of staff and officers to protect information they handle

2. Scope

This policy applies to all LPFA employees, officers, contractors, temporary staff, LPFA Board and Local Pension Board (LPB) members. It also applies to suppliers that provide third party services to LPFA, including where LPFA data, documentation or assets are utilised as either Joint Controllers or Processors or for any other service provided.

3. Responsibility

The LPFA Data Protection Officer (DPO) has overall responsibility for information management and security issues at LPFA.

Every member of staff is responsible for ensuring that any information held is accurate, remains confidential and secure and that the terms of this policy are adhered to.

LPFA's IT service provider is responsible for reviewing security event and error logs on a regular basis, and is responsible for downloading and installing any necessary software, security patches or system updates. The IT service provider is also responsible for its own information Security policy which it should ensure remains fit for purpose and compliant with the applicable legislation. LPFA is responsibility for ensuring oversight of its IT service provider in regard to adherence of service provision expectations and agreed service specifications and levels of performance.

4. Legal responsibilities

UK GDPR and the DPA 2018 impose requirements that:

- LPFA only holds data when it has a lawful basis for processing
- LPFA keeps that data confidential
- LPFA uses the data only for authorised purposes
- any data that LPFA holds is:
  - adequate
  - relevant
  - not excessive
  - accurate
  - up to date, and
  - not kept for longer than is necessary

5. Information Management

Records and information are owned by LPFA regardless that any individual or team may process such information. Keeping accurate and up-to-date records is an integral part of all business activities.

Complete and accurate records must be securely stored in the appropriate locations and be easily identifiable and accessible to those who need to see and use them.

This means:

- files must be kept in accordance with our normal file management protocols and must be kept organised and up to date
- personal data related emails must be saved securely and must not be stored solely in personal mailboxes
- documents must not be removed from the office except as permitted under this policy
- Information will be held only as long as is required and disposed of in accordance with our retention and disposal policy.
- All individuals must ensure that any information and data gathered is accurate and, where appropriate, kept up to date.

6. Information Security

Information Security requirements will continue to be aligned with LPFA's strategic objectives to with the aim of reducing information related risks to acceptable levels.

LPFA is committed to demonstrating to stakeholders that it has a robust approach to Information Security. It expects its third party service providers to meet industry accepted standards such as ISO 27001, and that they meet their regulatory requirements along with best practice in information security.

LPFA has set out the following high-level objectives to fully implement, continually strengthen and improve the Information Security approach taken and to ensure organisational excellence:

- Protect LPFA's business information and any information held by LPFA related to members, employers, employees or other stakeholders by maintaining its confidentiality, integrity and availability.
- Protect all information in line with any legal or regulatory requirements.
- Ensure maintenance of an appropriate level of awareness, knowledge and skill to allow the LPFA to minimise the occurrence and severity of information security incidents or data protection breaches.
- Ensure that third party service providers have information security key performance indicators (KPI's).
- Continue to work on any untreated risks, incidents and non-conformances through the monitoring and risk programmes

LPFA's Risk Management Principles provide the context for identifying, assessing, evaluating and controlling information-related risks both internally and with external service providers.

LPFA's Compliance Framework ensures all areas of the business that process personal data are regularly reviewed, assessed and evaluated to ensure compliance and for any future changes in UK GDPR or subsequent data protection legislation.

Other key areas that have a fundamental impact on information security are business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting. Control objectives for each of these areas are contained and supported by specific, documented policies and procedures.

7. Human resources information

Due to the internal confidentiality and sensitivity of personnel files, access to such information is limited to those who have responsibility for human resources within the organisation which may include those operating within a staff management capacity. Except as provided in individual roles, no other individuals are authorised to access that information.

Any staff member in a management or supervisory role must keep personnel information confidential.

Subject to the provisions of the UK GDPR and DPA 2018, individuals may ask to see their personnel files at any time. (See the subject access request within the Data Protection Policy).

8. Access to offices, working offsite and file storage

At the end of each day, whether working in the office or offsite, and when workspaces are unoccupied, all files, backup systems and devices containing confidential information must be securely stored. All office access doors must be kept secure at all times and clients and visitors must not be given keys or passcodes unless previously authorised.

Visitors should never be left alone in areas where they could have access to confidential information.

9. Computers and IT

Computers must be password protected and those passwords must be changed on a regular basis. Passwords should not be written down or given to others.

Computers and other devices should be locked when not in use to minimise the risk of accidental data loss or disclosure.

The use of memory sticks and other removable media is prohibited unless in exceptional circumstances where there is a justifiable reason to do so.

No confidential business and/or personal information is to be copied onto any removable data, for example, onto a removable hard drive, CD or DVD or memory stick, without the express permission of the Data Protection Officer and an LPFA Principal Officer. Any such authorised download of information must be to an encrypted device and be approved by the IT service provider.

Data copied to any of these devices should be deleted as soon as possible and stored on LPFA's computer network in order for it to be backed up.

10. Backup of data

All electronic data must be securely backed up by the IT service provider and in accordance with the agreed service specification in the Service Level Agreement.

11. Communication and transfer

Confidential information must not be removed from LPFA offices without permission from the relevant manager or except where that removal is temporary and necessary.

In such circumstances all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained.

This will include not:

- transporting documents in see-through or other un-secured bags or cases
- reading documents, information on laptops or tablets in public places where the personal data can be seen by someone else (waiting rooms, cafes, trains, etc)
- leaving documents unattended or in any place where they are at risk eg, in conference rooms, car boots, cafes or other such places.
- Postal, document exchange (DX), fax and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

- All sensitive or particularly confidential information should be encrypted before being sent by email or be sent by tracked DX or recorded delivery.
- Sensitive or particularly confidential information should not be sent by fax unless it can be confirmed that it will not be inappropriately intercepted at the recipient fax machine.

12. Personal email and cloud storage accounts

Personal email accounts, such as yahoo, google, hotmail and cloud storage services, such as dropbox, icloud and onedrive are vulnerable to hacking. They do not provide the same level of security as the services provided by LPFA's own IT systems.

- The use of personal email accounts or cloud storage account for work purposes, with the exception of LPFA and LPB board members, is prohibited, access has been disabled on the LPFA's network.
- If there is a need to transfer large amounts of data, advice must be sought from LPFA's IT service provider.

13. Home working

- No confidential or other information should be taken or stored at home to maintain the continued security and confidentiality of that information. With the approval of the Data Protection Officer and an LPFA Principal Officer, in exceptional justifiable circumstances, printed information may be held for temporary purposes but must be destroyed by secure disposal eg placed in the confidential waste bin at LPFA's offices or shredded using a cross-cut shredder so that no information is identifiable.
- No confidential information is to be stored on a home computer or device (PC, laptop, tablet or device). LPFA has the discretion to allow the use of "Bring your own devices" (BYODs) which are subject to a separate approval process and LPFA information is accessed through a separate portal.
- Laptops should be updated regularly and locked when unattended.

14. Overseas transfer

No overseas transfers of data can take place without the advice, guidance and approval by the Data Protection Officer. Any contracts with suppliers where data may be stored in other countries must not be agreed without the advice, guidance and approval of the Data Protection Officer.

LPFA's third party pensions administration provider may need to transfer data overseas, such as relating to those members residing in other countries. LPFA is responsible for ensuring that the pensions administration provider has the relevant safeguards in place to protect individual's data and to comply with its legal requirements.

15. IT system management and development

LPFA's IT system is managed by a third-party IT service provider who has a duty to ensure trained staff are responsible for overseeing day-to-day operation of LPFA's IT system and to ensure continued security and integrity.

As a minimum LPFA expects the service provider to:

- ensure all network devices have adequate protection e.g. up to date fire walls
- enable encryption of portable devices e.g. laptops, mobile phones etc
- ensure all devices require password protection

The service provider is responsible for the management of user accounts and will implement procedures to ensure:

- appropriate permissions are set for different types of user accounts, e.g. administration staff
- all members of staff have the correct type of user account
- users run with a minimal set of permissions whenever possible
- user accounts are suspended or deleted promptly where required, e.g. if a member of staff leaves LPFA

LPFA will set expectations regarding its security requirements through the Service Level Agreement held with the third-party service provider. This includes the prevention, detection and management of cybersecurity threats.

The People and Culture (P&C) team along with the IT service provider will ensure all access controls will be maintained at appropriate levels for all systems by ongoing and proactive management. Any changes to permissions must be approved by the relevant manager.

16. Business continuity

Please refer to LPFA's Business Continuity plan. This has been designed to ensure continued data security and to maintain confidentiality.

17. Reporting breaches

All individuals who are subject to this policy have an obligation to report actual or potential data protection/information security compliance failures in line with the Data Protection Policy process and this policy.

This allows LPFA to:

- investigate the failure and take remedial steps if necessary
- maintain a register of compliance failures
- notify the ICO of serious compliance failures

Refer to LPFA's data protection reporting procedure. In the event of a potential or actual cybersecurity event, the Data Protection Officer and the third-party IT service provider must be notified immediately after the individual becomes aware of the risk.

18. Training

All employees will receive LPFA's Acceptable Computer Usage policy and be required to complete compulsory e-learning on data protection and information security. New joiners will receive this as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or LPFA's policy and procedure.

Training is provided online via LPFA's training platform and through 'lunch and learns' and via other appropriate training mediums including self-directed training.

Completion of training is compulsory.

The Data Protection Officer will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or any of this policy please contact the LPFA Compliance and Regulation Manager.

19. Monitoring

Everyone must observe this policy. The Data Protection Officer, having overall responsibility for this policy, will monitor adherence to this policy.

20. Consequences of failing to comply

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action.

If you have any questions or concerns about anything in this policy, please contact the LPFA Compliance and Regulation Manager in the first instance.

21. Policy Review

This policy will be reviewed periodically as stated in the LPFA Policy Framework.