Public Sector
Audit Appointments

Information governance policy

July 2020

Contents

Introduction 2
Legal compliance 2
Risk management 2
Information security 3
Information assets 3
Audit firms 4
Secure file transfer 4
Information and records management 4
CRM system 5
Document retention and destruction policy 5
Roles and responsibilities 5
Related policies 7

Introduction

1 The aim of PSAA's information governance policy is to ensure that the company is meeting its compliance obligations under data protection requirements and the Freedom of Information Act, and is adhering to best practice principles on information management.

2 The policy seeks to ensure that:

- information is protected against unauthorised access;
- confidentiality of information is assured;
- integrity of information is maintained;
- regulatory and legislative requirements are met; and
- all breaches of information security, actual or suspected are reported to senior management.

3 The policy is relevant to all PSAA staff (including temporary and contract staff) who create, store, share and dispose of personal and business sensitive information. Though many of the controls are concerned with the management of electronic information and associated systems, the framework also covers paper records.

4 PSAA staff (including temporary and contract staff) must also comply with:

- the Code of Conduct, which sets out the standards of conduct and behaviour the company requires; and
- the related data protection, information management and freedom of information policies (listed at paragraph 35 of this document).

Legal compliance

5 The purpose of the Freedom of Information Act 2000 (FOIA) is to promote greater openness by public authorities and availability of information. PSAA as a wholly owned subsidiary of IDeA (which in turn is a wholly owned subsidiary of the LGA) is subject to the provisions of the FOIA and is therefore required to comply with requests for information. We endeavour to publish as much information on our website as we can.

6 Appointed auditors exercise separate statutory powers to PSAA and are not subject to the FOIA. See the FOI page on the PSAA website for more information.

7 The General Data Protection Regulation (GDPR) imposes statutory obligations on anybody processing personal data. PSAA is legally responsible for ensuring that any personal information it creates, collects, uses, stores or otherwise processes must be handled and protected in accordance with GDPR requirements. PSAA staff must adhere to the PSAA data protection policy and the LGA policies and guidance.

Risk management

8 Using information well helps to make our business more efficient and improves the services we offer. The risks in handling information are not only in failing to protect it properly, but also in not using it in the right way. Managing information risk is about taking a proportionate approach

so that these aims are achieved. Our approach to information risk management is covered by PSAA's corporate risk management strategy and policy.

Information security

9 PSAA is included in the LGA’s ICT contract and is subject to the LGA’s ICT usage and security policy. The policy sets out the LGA’s rules and procedures for use of ICT equipment, systems and data.

10 PSAA operates a clear desk and clear screen policy. When desks are unoccupied it is expected that any personal or business sensitive information is locked away in lockers as appropriate and screens should be left in ‘lock’ mode.

11 All PSAA staff have access to files stored in the S: drive. The only restriction on access is to S:\Corporate management\Finance and all associated sub-folders which are restricted to PSAA management team members plus the Finance Manager.

Information assets

12 PSAA recognises a number of information asset categories that are central to the efficient running of the business. Our priority is the protection of information assets which comprise personal and business sensitive information, for example information relating to audited bodies, personnel and finance. This includes electronic data held in ICT systems and equipment, or paper documents held in our care.

13 Information assets are documented in PSAA's information asset register and each is assigned an information asset owner. The purpose of the register is to record the business areas and processes which handle personal and business sensitive information.

14 It is important that the register is kept under control and updated as necessary. The register should be updated every time the details of one of the assets are changed.

15 PSAA’s information is a fundamentally important business asset. It is essential that its confidentiality and integrity is suitably protected. PSAA’s information falls into one of the following categories:

- Financial
- Employee-related
- Legal/contractual
- Governance
- Operational
- Audited body and stakeholder information
- LAQF
- Website
- Intranet

16 PSAA has a service-level agreement with the LGA to provide company secretarial, payroll, HR, IT and financial services.

Audit firms

17 Specific arrangements are in place with partner audit firms to ensure that information risks are managed, and firms comply with PSAA's contract terms and policies. On an annual basis the audit firms are asked to provide details of their information governance and data security arrangements including details of any data breaches by updating their ITT submissions. On occasions internal audit may be asked to review and check the assurances provided by the audit firms in these submissions

Secure file transfer

18 The secure file transfer system (Egress) is a web-based system for sending and receiving files securely to and from external organisations and individuals. Egress should be used for the transfer of confidential and sensitive information. Documents are uploaded to the system and an email with a link to Egress is sent to the recipient. Documents can only be accessed by signing up to Egress and setting up a password access.

Information and records management

19 In general, documents should be stored electronically. Individuals may choose to keep a small number of documents in hard copy for personal reference but should always be mindful of security issues. Confidential documents should be locked away and those held in hard copy kept to a minimum.

20 The main categories of secure information assets held by PSAA are:

- employee information;
- financial information;
- contact information required to discharge statutory responsibilities; and
- legal and contract documents.

21 All electronic data should be stored on the PSAA network on one of the following drives:

- H drive: personal drive for each member of staff to store information that should not be accessed by other team members, for example records of performance discussions;
- S drive: shared drive containing PSAA's business information with access to the Finance folders restricted; and
- CRM system: database containing all information on audited bodies.

22 Data should not be stored on laptop C drives (including the desktop) as it is not backed up. If laptops are lost or stolen or the hard drive corrupts data, it will not be possible to retrieve data on the C drive.

23 Emails are part of the formal record-keeping of PSAA and should be written in a professional and objective manner. Emails that need to be retained should be stored in folders

either in Outlook, in the CRM system, or in the relevant folder on the shared S drive. Emails, including those that have been deleted, can be retrieved via Mimecast.

CRM system

24 The CRM system contains comprehensive information about audited bodies, including contact details for opted-in bodies, their appointed auditors, and PSAA's other key stakeholders. It is reviewed and updated regularly, including through information returns submitted by the audit firms.

25 The CRM system is used to manage auditor appointments and to produce contact lists for mailings. The system is the prime source of PSAA data on audited bodies. Data should only be downloaded from the system for a specific purpose and stored securely.

Document retention and destruction policy

26 In line with best practice, an information audit will be undertaken every two years, with information reviewed and deleted according to the requirements of the PSAA retention and disposal schedule.

27 PSAA staff should implement the following best practice general principles:

- all data should be kept in line with agreed policies;
- data considered to be obsolete should be destroyed;
- data needed for reference purposes only should be archived;
- duplicate records or older versions of the same documents should be deleted at an appropriate stage;
- sensitive information held in hard copy should be destroyed securely by shredding or placing in sealed confidential waste bags; and
- original signed contracts should be held securely.

28 PSAA staff should review their mailbox by following the best practice principles:

- regularly clean out your Inbox and its subfolders and your Sent items folder;
- regularly empty your trash folder;
- adopt an attachment management strategy – decide if and how you will save attachments to ensure you can locate them easily; and
- save business critical emails in the relevant folder on the shared S: drive.

Roles and responsibilities

29 Everyone who works for or with PSAA has some responsibility for ensuring data is collected, stored, handled and processed appropriately in line with PSAA policies relating to information governance and the data protection principles.

30 The PSAA board of directors is ultimately responsible for ensuring that PSAA meets its legal obligations.

31 The Chief Executive is the nominated data protection lead officer so is responsible for the overall management of information for PSAA.

32 The Senior Information Risk Officer (SIRO) is a manager who is familiar with information risks and the organisation's response. This role is assigned to the Chief Financial Officer. The SIRO's responsibilities are to be the lead for PSAA on managing information risk and update the Chief Executive on information governance issues. Specific responsibilities include:

- keeping up-to-date with latest developments in relation to data protection/information governance law and their implications for PSAA, and updating the Board about data protection/information governance responsibilities, risks and issues;
- identifying areas where there is the risk of a data protection breach;
- advising on DPA breaches and referring serious breaches to the ICO.
- Monitoring and reviewing all data protection procedures and related DP and information governance policies, interpretation of requirements and checking compliance;
- arranging data protection training and advice for the people covered by this policy;
- handling data protection questions from staff and anyone else covered by this policy;
- dealing with requests from individuals to see the data PSAA holds about them (also called 'subject access requests'), to exercise their rights in relation to data held about them by PSAA (called 'individual's rights requests') and approving unusual or controversial disclosures of data;
- checking and approving any contracts or agreements with third parties that may handle the company's sensitive data;
- regularly reviewing and updating PSAA's registration with the ICO;
- approving any data protection statements attached to communications such as emails and letters;
- addressing any data protection queries from journalists or media outlets like newspapers; and
- where necessary, working with other staff to ensure communications and marketing initiatives abide by data protection principles.

33 Information asset owners are responsible for the effective management of their team's information, including implementation of and compliance with this policy and related policies. They are responsible for:

- ensuring information is appropriately classified;
- ensuring all documents are being stored in accordance with this policy;
- ensuring that team members understand and follow the PSAA policies and procedures in relation to information management;
- approving appropriate data access;
- defining and periodically reviewing access restrictions and classifications; and
- ensuring that PSAA's procedures are applied when employees join, change their status, or leave the organisation.

34 It is the responsibility of all PSAA staff to:

- understand and comply with this policy and related policies (see below);

- maintain the confidentiality of PSAA’s information;
- comply with PSAA’s Code of Conduct;
- ensure that information is only used for authorised purposes;
- protect information from disclosure, corruption and loss; and
- undertake mandatory annual e-learning training on data protection and information governance.

Related policies

35 The following set out requirements related to this information governance policy:

- PSAA data protection policy;
- PSAA data privacy notice;
- PSAA data breach incident response plan;
- PSAA information asset register;
- Freedom of Information Policy and Staff procedure; and
- the LGA ICT usage and security policy.