Data Protection Policy

Owned and maintained by:	Corporate Governance Manager				
Approved from:	September 2016	**Next review:**	August 2017	**Version:**	11

Introduction

1. The Data Protection Act 1998 (DPA) places a duty on us to protect the personal information that we collect and hold and to provide individuals with access to the personal information we possess about them.

2. Audit Scotland collects and processes personal information covered by the DPA. Examples include information on current, past and prospective employees, clients, suppliers, complainants, people covered by the audit process and others with whom we communicate.

3. Audit Scotland recognises the benefits of the DPA for both the organisation and the individual (data subject), and the seriousness of failing to comply with it and the risk of prosecution. Therefore, we are committed to:
   - full staff awareness and on-going training in data protection legislation, its implications for our work, our data protection arrangements and our data loss/incident process
   - ensuring that all personal information is stored and processed properly and securely in keeping with the eight data protection principles
   - implementing effective systems for handling data subject access requests (requests from individuals to access their personal information)
   - implementing effective systems for handling security breaches and data loss.

Scope

4. This policy applies to the Auditor General, the Accounts Commission and Audit Scotland.

5. This policy does not cover personal information stored on our network by any other organisation as part of a shared service agreement.

6. Data-matching exercises as part of the National Fraud Initiative are subject to a detailed Code of Data-Matching Practice which complies with this policy.

Definition

7. The DPA defines personal data as information about a living, identifiable individual and requires that all personal data is stored securely and processed properly. It applies to information held on paper, on a computer, or stored on any other medium.

Principles

8. The DPA contains eight data protection principles which specify the standards that must be met when obtaining, handling, processing, transporting and storing personal data. We are committed to these principles.

9. To comply with the eight data protection principles we will:

   9.1. collect and process personal information fairly and lawfully

   9.2. collect, store and process personal information only for the purposes originally specified, which must fall within our remit

   9.3. ensure that personal information we collect, store and process is confined to what is required for our purposes and is not disclosed improperly

   9.4. ensure the accuracy of personal information and, where necessary, keep the information up to date

   9.5. destroy personal information when it is no longer needed for the purpose it was originally collected

   9.6. process personal information in accordance with the rights of data subjects and ensure that any data subject access requests and rights are handled fairly, courteously and completed within 40 days of a valid request

   9.7. protect the personal information we collect, process, store and transport from unauthorised access, abuse, loss or damage by providing appropriate security, both technical and organisational

   9.8. ensure that personal information is not transferred to people or other organisations outside the European Economic Area.

Disclosure of personal information

10. We will supply personal information to:
    - those who are entitled to the information
    - any authority we are required to do so by law eg HMRC
    - anyone to whom we are required to disclose it, such as staff seeking to access their own personal data.

Roles, responsibilities and governance arrangements

11. The Corporate Governance Manager's role is to:
    - maintain and update the data protection register for Audit Scotland, the Auditor General and the Accounts Commission
    - manage any data subject access requests
    - manage any data security breaches or data loss incidents

- provide advice and assistance for staff on data protection issues and where necessary commission legal advice
- provide data protection training and guidance for staff
- maintain and update the data protection policy and associated documentation
- advise the management team on compliance with the DPA
- manage personal data audits if required by the management team.

12. Figure 1 shows the reporting arrangements. The Corporate Governance Manager (CGM) reports directly to the Chief Operating Officer and attends the meetings of the Knowledge, Information & Technology Governance Group (KITGG).

13. The KITGG is responsible for overseeing and developing our data protection arrangements and presenting them to Audit Scotland's management team and/or Board/Audit Committee for approval.

14. You can contact the CGM at dataprotection@audit-scotland.gov.uk

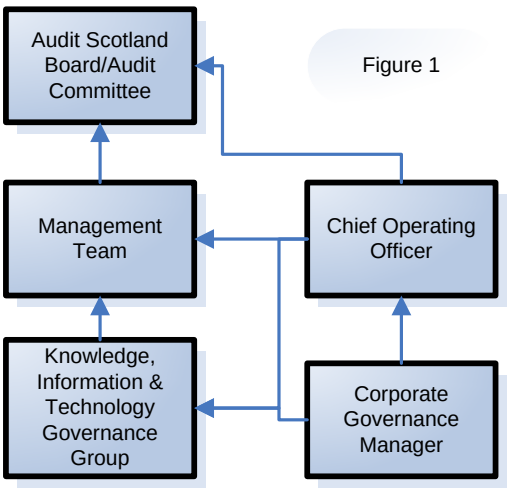

Figure 1

15. Data protection is the responsibility of everyone and this principle is embedded in our Code of Conduct. We are all expected to ensure that we collect, process, store, share and dispose of personal data in accordance with this policy and the Data Protection Act, and to under go training as required.

Training and awareness

16. We are committed to full staff awareness and training in Data Protection, Freedom of Information and Environmental Information Regulations legislation and its implications for our work. We are committed to maintaining effective systems for handling personal data to meet our obligations under this legislation.

17. Guidance on the application of data protection is available on ishare.

Misuse of employee and audit data

18. It is an offence under the DPA for staff to disclose personal data of others to third parties or procure the disclosing of such personal data to third parties without the consent of Audit Scotland. This includes personal information we hold as a result of our audit work.

19. Failure of staff to comply with this policy and the eight data protection principles may result in action under Audit Scotland's disciplinary policy and could incur a risk of personal prosecution.

Supplementary documentation

20. The following Acts, policies, standards, procedures and guides should be used to support and supplement this policy:

- Data Protection Act 1998.
- The personal data checklist (see Appendix 1), which enables staff to identify if information is covered by the DPA.
- The data subject access procedure, which defines the process to be followed for a data subject access request.
- The data loss procedure, which defines the process to be followed for a data security breach or loss of data.

21. Current versions of these documents can be found on Audit Scotland's intranet – ishare.

Appendix 1 - Personal data checklist

Use this flow chart to help you decide if the information you hold is personal data and therefore covered by the Data Protection Act.