

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

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

Audit Scotland recognises the benefits of the DPA for both organisation and data subject, and the seriousness of failing to comply with the DPA and the risk of prosecution. Therefore, we are committed to:

- full staff awareness and ongoing training in data protection legislation and its implications for our work
- 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

This policy applies to the Auditor General, the Accounts Commission and Audit Scotland, their employees including temporary staff, students and organisations acting on their behalf.

This policy does not cover personal information stored on our network by the Sustainable Development Commission. 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.

## Principles

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.

To comply with the eight data protection principles we will:

1. collect and process personal information fairly and lawfully
2. collect, store and process personal information only for the purposes originally specified, which must fall within our remit
3. ensure that personal information we collect, store and process is confined to what is required for our purposes and is not disclosed improperly
4. ensure the accuracy of personal information and, where necessary, keep the information up to date
5. destroy personal information when it is no longer needed for the purpose it was originally collected
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
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
8. ensure that personal information is not transferred to people or other organisations outside the European Economic Area.

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.

### The data protection officer's role and governance arrangements

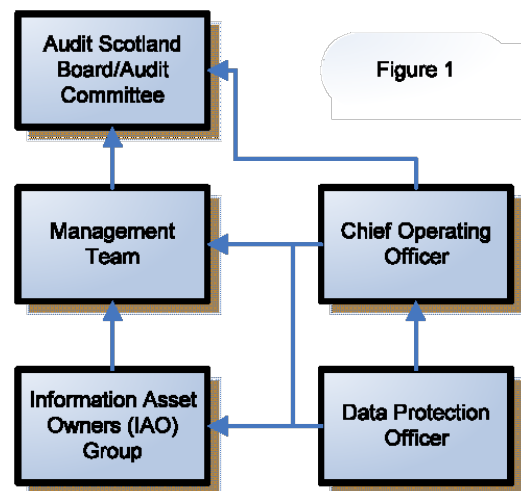
The data protection officer's role is to:

- maintain and update the data protection register for Audit Scotland, the Auditor General and the Accounts Commission
- manage any data subject access requests
- assist in 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.

Figure 1 shows the reporting arrangements. The data protection officer reports directly to the Chief Operating Officer and attends the meetings of the Information Asset Owners Group.

The Information Asset Owners Group 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.

You can contact the DPO at [dataprotection@audit-scotland.gov.uk](mailto:dataprotection@audit-scotland.gov.uk)



### Supplementary documentation

The following documents should be used to support and supplement this policy:

- 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.

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

## 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.

