Data Protection Policy

Owned and maintained by:	Corporate Governance Manager				
Approved from:	May 2018	**Next review:**	April 2019	**Version:**	13

Introduction

1. This Data Protection policy applies to the Auditor General, the Accounts Commission and Audit Scotland. Throughout this policy the terms 'we' and 'us' are used to refer to the Auditor General, the Accounts Commission and Audit Scotland collectively.

2. As Data Controllers, we are committed to processing personal data (information) lawfully, fairly and in a transparent manner.

3. To discharge our statutory functions we collect, process, store and delete personal information covered by data protection legislation. Examples include information on current, past and prospective employees, Accounts Commission members' and previous Auditor Generals, clients, suppliers, correspondents, complainants, people covered by the audit process and others with whom we communicate.

4. We recognise the benefits of protecting an individual's fundamental rights and freedoms and in particular their right to the protection of their personal information. We also recognise the seriousness of failing to comply with data protection legislation and the resulting risk to our reputation. Therefore, we are committed to:

    4.1. ensuring that all personal information is processed lawfully and in compliance current data protection legislation

    4.2. ensuring that our digital systems are secure and that personal information will be stored securely

    4.3. implementing effective systems for ensuring the rights of individuals, such as systems for handling and responding to data subject access requests within one month or receipt (requests from individuals to access their personal information)

    4.4. designing systems, processes and methods of working that protect personal information entrusted to us (privacy by design and default)

    4.5. undertaking data protection impact assessments as necessary for major new projects or when considering new software

    4.6. full awareness of and on-going training in data protection legislation, its implications for our work, our data protection arrangements and our data loss/incident process

    4.7. implementing effective systems for handling security breaches and data loss.

5. 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

6. Personal data is defined as *'any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'*.

7. It applies only to living individuals and covers their personal information held on physical or digital medium.

Data protection principles

8. The EU 2016/679 General Data Protection Regulation (GDPR) contains six principles for processing personal information. They specify the standards that must be met when obtaining, handling, processing, transporting and storing personal information. We will only process personal information where we have a lawful purpose for doing so.

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

    9.1. process personal information lawfully, fairly and in a transparent manager in relation to the data subject

    9.2. only collect personal information for specified, explicit and legitimate purposes and not further process it in a manner that is incompatible with those purposes

    9.3. ensure that the personal information we collect is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

    9.4. ensure the accuracy of personal information and, where necessary, keep the information up to date; personal information that is inaccurate will be erased or rectified without delay

    9.5. only keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes

    9.6. ensure personal information is only processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Disclosure of personal information

10. We will only disclose personal information to:

    10.1. those who are entitled to the information

    10.2. any authority we are required to do so by law eg HMRC

    10.3. anyone to whom we are required to disclose it, such as individuals seeking to access their own personal data.

Data protection officer

11. The Corporate Governance Manager is our designated data protection officer. He is to be involved, properly and in a timely manner, in all issues which relate to the protection of personal information.

Personal responsibility

12. 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 a fair and lawful manner, in accordance with this policy and data protection legislation, and to under go training as required.

Training and awareness

13. We are committed to full staff awareness and training in Data Protection, Information Security, 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.

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

Misuse of personal information

15. Failure of staff to comply with this policy and the data protection principles may result in action under Audit Scotland's disciplinary policy.

Change log

Version	Date	Author	Description
13	12/04/2018	Corporate Governance Manager	Data protection policy changed to include GDPR requirements and the commencement of this change log.