Data Protection Policy

Owned and maintained by:	Corporate Governance Manager				
Approved from:	May 2019	**Next review:**	April 2020	**Version:**	14

Introduction

1. The Data Protection Act (DPA) 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018.

2. It sits alongside the GDPR, and tailors how the GDPR applies in the UK - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

3. The frameworks are comprehensive and apply tough punishments for non-compliance with rules around the storage and handling of personal data.

4. 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.

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

6. 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 Auditors General, clients, suppliers, correspondents, complainants, people covered by the audit process and others with whom we communicate.

7. 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:

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

    7.2. ensuring that our digital systems are secure, and that personal information will be stored securely;

    7.3. 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);

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

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

7.6. 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;

7.7. implementing effective systems for handling security breaches and data losses;

7.8. ensuring that when we use a data processor that a written contract is in place so that both parties understand their responsibilities and liabilities;

7.9. ensuring that any data processor we use also implements appropriate technical and organisational measures;

7.10. conducting regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement;

7.11. understanding that encryption can be an appropriate technical measure to ensure that we process personal data securely;

7.12. ensuring that we keep our encryption solution(s) under review in the light of technological developments.

8. 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

9. 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'*.

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

Data protection principles

11. The EU 2016/679 General Data Protection Regulation (GDPR) contains seven principles for processing personal information. They specify the standards that must be met when obtaining, handling, processing, transporting and storing personal information. The seven data protection principles are listed below:

11.1. Lawfulness, fairness and transparency;

11.2. Purpose limitation;

11.3. Data minimisation;

11.4. Accuracy;

11.5. Storage limitation;

11.6. Integrity and confidentiality (security); and

11.7. Accountability

12. In line with these principles, we will only process personal information where we have a lawful purpose for doing so, and be cognisant of rules relating to exemptions that apply.

13. To comply with the seven data protection principles, we will:

13.1. process personal information lawfully, fairly and in a transparent manner in relation to the data subject;

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

13.3. 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;

13.4. 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;

13.5. 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;

13.6. 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'); and

13.7. ensure that we can demonstrate compliance with GDPR regulations by being able to evidence the steps we have taken to secure personal data including removal / redaction. We require to have a process in place to manage any requests, but also need to have a full audit trail to prove that we undertook the proper actions.

Disclosure of personal information

14. We will only disclose personal information to:

14.1. those who are entitled to the information;

14.2. any authority we are required to do so by law e.g. HMRC; and

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

Rights of the individual

15. The GDPR provides the following rights for individuals which we as an organisation must be cognisant of:

15.1. The right to be informed - this covers some of the key transparency requirements of the GDPR. It is about providing individuals with clear and concise information about what you do with their personal data. Articles 13 and 14 of the GDPR specify what individuals have the right to be informed about.

15.2. The right of access - this is commonly referred to as subject access and gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

15.3. The right to rectification - Under Article 16 of the GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

15.4. The right to erasure - Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

15.5. The right to restrict processing - Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely but will need to have the restriction in place for a certain period of time.

15.6. The right to data portability - The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

15.7. The right to object - Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask you to stop processing their personal data. The right to object only applies in certain circumstances.

Whether it applies depends on your purposes for processing and your lawful basis for processing.

15.8. Rights in relation to automated decision making and profiling - Under Article 4 (4) any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Data protection officer

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

Personal responsibility

17. 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 undergo training as required.

Training and awareness

18. 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.

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

Misuse of personal information

20. 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.
14	26/03/2019	Corporate Governance Manager	Updated to reflect the further guidance updates on GDPR since April 2018
15	01/05/19	Corporate Governance Manager	Revised policy approved by Audit Scotland Board