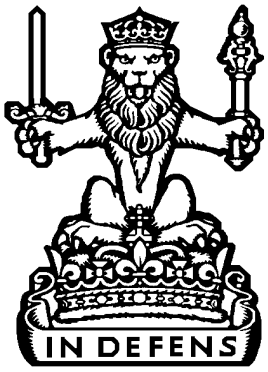
DATA PROTECTION MANUAL



Approvals and Date for Review

Approval	Date	Further Approval	Date	Actions/Review Due
Head of Policy	August 2008	Crown Agent and Chief Executive	September 2008	June 2015
Records Management Board	May 2015	Crown Agent and Chief Executive	June 2015	Updated for NRS October 2015
Records Management Board	October 2015	Crown Agent and Chief Executive	October 2015	June 2016
Policy Division	October 2016	N/A – minor amendment to Annex B	October 2016	October 2017

CONTENTS

Part A: General Guidance

1	Introduction to the Data Protection Act 1998	5
2	The Data Protection Principles	9
3	Personal Data & Relevant Filing Systems	15
4	Rights of the Individual under the Data Protection Act 1998	22
5	Exemptions: General Principles	26
6	Categories of Exemptions	29
7	Freedom of Information (Scotland) Act 2002 & the Environmental Information Regulations	35
8	The Role of the Information Commissioner	36

Part B: Applying the Data Protection Act within COPFS

9	Applying Exemptions to the Subject Information Provisions	38
10	Data Sharing of Personal Data & Applying the Exemptions	41
11	Requests for Data Sharing	46
12	Subject Access Requests	51
13	Information Relating to another Individual	57
14	Offences under the Data Protection Act 1998	60

Annexes

A	Definitions & Key Concepts	63
B	Sample Subject Access Request Form	66
C	Style Paragraphs	68
D	Comparative Rights of Access under the DPA 1998 and the FOI(S)A 2002	69

E Subject Access Requests Flowchart 73

PART A: GENERAL GUIDANCE

Chapter 1: Introduction

1.1 Background to the Data Protection Act 1998

1.1.1 The Data Protection Act 1998 (the 1998 Act) came into force on 1 March 2000 and replaced the Data Protection Act 1984. The 1998 Act implements EC Directive 95/46/EC which was adopted in October 1995. The aim of the Directive is to harmonise data protection law among member states and its objectives are detailed in Article 1:

> *"In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."*

1.1.2 The 1998 Act aims to achieve this objective in **two** ways:

a) It imposes **duties** on anyone who processes personal information ("data controllers") to comply with the eight principles of good information handling set out in **Schedule 1** of the 1998 Act ("the Data Protection Principles");

b) It gives **rights** to individuals ("data subjects"), including the right to know what information is held about them.

1.1.3 The provisions and extended definitions of the 1998 Act substantially broadened the impact of the data protection regime. In particular, the 1984 Act only applied to electronic data held about individuals whereas the 1998 Act applies to all data, including manual records held within relevant filing systems.

1.2 The Data Protection Principles

1.2.1 The 8 Data Protection Principles are set out in **Schedule 1** of the 1998 Act and ensure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the individual's rights
- Secure
- Not transferred to other countries without adequate protection.

1.2.2 **Part II** of **Schedule 1** provides the interpretation provisions which expand upon the First, Second, Fourth, Sixth, Seventh and Eighth principles.

1.2.3 Subject to any exemptions afforded by **sections 27-39** of the 1998 Act, the data controller (e.g. COPFS) has a duty to comply with the 8 Data Protection principles.

1.2.4 Further information and guidance on the 8 Data Protection Principles are provided in Chapter 2 of this Manual.

1.3 Subject Access Requests

1.3.1 **Section 7** of the 1998 Act entitles an individual to request a copy of information constituting personal data held by a data controller. This is called a Subject Access Request (SAR). This right is subject to a number of exemptions in **Part IV** and **Schedule 7** of the 1998 Act and these are considered at Chapters 5, 6, 9 and 10 of this Manual.

1.3.2 Subject to exemption, when an individual makes an SAR they are entitled to:

a) be informed whether personal information about them is being processed by the data controller;
b) be given a description of any such information;
c) be advised of the purposes for which that information is being processed;
d) be advised of the people to whom the information may be disclosed; and
e) have the content of the information communicated to them and to be told of the source of the information if known.

1.3.3 The 1998 Act does not confer any right of access to a third party's personal data. However the exemptions do operate to permit data sharing in certain limited circumstances. Further guidance on this is set out in Chapter 10 of this Manual.

1.4 Information regulated by the 1998 Act

1.4.1 The 1998 Act applies to the "processing" of "personal data" and "sensitive personal data". These concepts are defined in **Sections 1** and **2** of the 1998 Act.

1.4.2 "**Processing**" is a broad term which incorporates all use of data - from creation, retrieval and disclosure to other more passive treatments, including storage. When carrying out any of those processes all staff must ensure that the data are handled in accordance with the data protection principles.

1.4.3 "**Personal data**" is defined as **data** which **relates** to a **living individual** who can be **identified**-

a) from the data, or
b) from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

1.4.4 This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

1.4.5 "**Sensitive personal data**" is personal data with particular content, for example the data subject's racial background or political opinions.

1.4.6 "**Data**" can be held **manually** or **electronically** and so far as public authorities (e.g. COPFS) are concerned the definition includes virtually all data held in all formats.

1.4.7 Identifying whether information is "personal data" is crucial to the application of the legislation and is examined in more detail at Chapter 3 of this Manual.

1.4.8 The Definitions set out in **Sections 1** and **2** of the 1998 Act are contained in Annex A to this Manual.

1.5 Data Protection Responsibilities within COPFS

1.5.1 The Response & Information Unit (RIU), Policy Division, Crown Office, has responsibility for co-ordinating compliance and responding to all requests for personal information under the Data Protection Act.

1.5.2 – Persons seeking their own personal information should be provided with the subject access request application form (insert link to http://www.copfs.gov.uk/images/Documents/Prosecution_Policy_Guidance/Guidelines_and_Policy/Subject%20Access%20Request%20form%202014.pdf) and should be asked to submit it to the RIU Team through the _Subject Access Requests mailbox.

1.6 Information held by COPFS

1.6.1 A substantial part of the information held by COPFS is information held and obtained by the Crown in connection with the prevention and detection of crime, or the apprehension and prosecution of offenders and should only be disclosed in the following circumstances:

- For the purposes for which the information was imparted; and/or
- If the disclosure of such information is in accordance with a statutory duty or a common law authority.

1.6.2 There are therefore difficulties envisaged in disclosing information for purposes out with the core functions of the COPFS, the most obvious examples being for the purposes of civil proceedings, to the Criminal Injuries Compensation Authority, to witness support services and to regulatory bodies where there is no statutory disclosure regime in place.

1.7 COPFS as a Data Controller

1.7.1 Within the terms of the 1998 Act, the data controller is the person or body with the ultimate authority and responsibility for determining the purposes and means of processing the personal data within their control.

1.7.2 In terms of **Section 7** of the 1998 Act, data controllers must (unless exempt) notify the Information Commissioner's Office and provide them with certain "registrable particulars."

1.7.3 COPFS is a registered data controller and has a notification lodged with the Information Commissioner to the effect that the organisation holds and processes data for five purposes:

(1) Staff Administration
(2) Accounts & Records
(3) Investigation of sudden, suspicious and unexplained deaths
(4) Advertising, marketing and public relations
(5) Crime Prevention and prosecution of offenders

1.7.4 COPFS is also a Scottish Public Authority under the Freedom of Information (Scotland) Act 2002.

1.8 The Role of the Information Commissioner

1.8.1 Whereas the Scottish Information Commissioner has responsibility for compliance with Freedom of Information legislation, it is the Information Commissioner (for the UK) who oversees the operation of the Data Protection Act 1998.

1.8.2 In particular the Information Commissioner has the responsibility to:

- Promote the following of good practice and disseminate information about the Act;
- Maintain a register of persons who have given notification;
- Enforce the terms of the Act and investigate alleged breaches and respond to non-compliance

1.8.3 Further guidance on the role and responsibilities of the Information Commissioner are contained in Chapter 8 of this Manual.

Chapter 2: The Data Protection Principles

2.1 First Principle

2.1.1 The first principle provides that "**personal data shall be processed fairly and lawfully** and, in particular, shall not be processed unless—

(a) At least one of the conditions in **Schedule 2** is met, and
(b) In the case of sensitive personal data, at least one of the conditions in **Schedule 3** is also met".

2.1.2 It is important to note, however, that meeting a **Schedule 2** and a **Schedule 3** condition will not, in itself, ensure that the processing of the personal data is fair and lawful.

"Processed Fairly"

2.1.3 The data should be processed **fairly** and this is defined in **Schedule 1, Part II, Paragraphs 1-4**. Fairness demands that the data subject was not deceived or misled as to the purpose of the processing.

2.1.4 The data controller should, as far as practicable, make the following information available to the data subject:

a) The identity of the data controller;
b) If the data controller has nominated a representative for the purposes of the Act, the identity of that representative;
c) The purpose or purposes for which the data are intended to be processed; and
d) Any further information which is necessary to enable fair processing.

2.1.5 When determining what, if any, further information is required (under sub-paragraph (d) above), data, the data controller should consider what processing of personal data they will be carrying out once that data has been obtained and then consider whether the data subject is likely to understand:

(a) The purposes for which their personal data will be processed;
(b) The likely consequences of such processing such that the data subject is able to make a judgments as to the nature and extent of the processing; and
(c) Whether particular disclosures can reasonably be envisaged.

2.1.6 This information should be provided when the data are first processed, at a time soon after disclosure has been made or at a time when disclosure to a third party is contemplated.

"Processed Lawfully"

2.1.7 The 1998 Act does not provide an interpretation on the meaning of "lawful" but the Courts have broadly described unlawful to mean "something which is contrary to some law or enactment or is done without lawful justification or excuse"[1]. To be processed **lawfully**, therefore the data controller must comply with statutory and common law obligations, for example duties of confidence owed to a third party and ECHR obligations, in particular the Article 8 right to privacy. Lawful processing is a pre-requisite of the first data protection principle and the Act cannot render unlawful processing lawful, even where the processing complies with the data protection principles.

2.1.8 In order to ensure that the data controller is acting **lawfully**, it is essential that the data controller is aware of the extent of their powers. COPFS deals with personal data in order to carry out specific functions and if personal data is processed outside these functions then the processing may be deemed to be unlawful.

2.1.9 Once the conditions of fair and lawful treatment have been satisfied, one condition in **Schedule 2** (and one condition in **Schedule 3** in the case of sensitive personal data) must also be satisfied to comply with the first data protection principle.

2.1.10 In terms of **Schedule 2** at least one of the following conditions must be met for personal information to be considered lawfully and fairly processed:

a) The individual has consented to the processing;
b) Processing is necessary for the performance of a contract with the individual;
c) Processing is required under a legal obligation (other than one imposed by the contract);
d) Processing is necessary to protect the vital interests of the individual;
e) Processing is necessary to carry out public functions, e.g. administration of justice; or
f) Processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could unjustifiably prejudice the interests of the individual).

Sensitive Personal Information

2.1.11 Specific provision is made for processing sensitive personal information, and at least one additional condition detailed in **Schedule 3** must be met to comply with the first data protection principle. These are:

a) Having the explicit consent of the individual;

[1] *R v R* [1991] 4 All ER 481

b) Processing necessary for the purpose of exercising or performing a legal right or obligation in the context of employment;
c) Needing to process the information in order to protect the vital interests of the individual or another person;
d) Processing of political, philosophical, religious or trade union data in connection with its legitimate interests by any non-profit bodies;
e) Processing of information made public as a result of steps deliberately taken by the data subject;
f) Dealing with the administration of justice or legal proceedings;
g) Processing necessary for the administration of justice, the performance of statutory functions, exercise of function of the Crown, Ministers or government departments;
h) Processing of medical data by medical professionals or others owing an obligation of confidence to the data subject; or
i) Ethnic monitoring.

Consent

2.1.12 Consent is not defined in the Act and, accordingly, the existence of consent must be assessed in the light of the facts. The European Data Protective Directive defines "the data subject's consent" as *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".*

2.1.13 In effect, therefore, there must be active communication between the data subject and the data controller, but need not be in writing.

2.1.14 Data controllers, however, cannot infer consent from a negative response, e.g. a person's failure to return or respond to correspondence. Although it may not amount to consent, however, it **may** provide the data controller with the basis to rely upon another **Schedule 2** condition, e.g. legitimate interest condition, provides that the data subject is given the right to object before the data is obtained.

2.1.15 Consent on the basis of misleading information or consent obtained under duress will not be valid basis for processing.

2.1.16 Where the consent is to the processing of sensitive data, then the consent **must** be explicit, i.e. the terms of the consent of the data subject should be absolutely clear and should usually cover the specific detail of the processing, the particular type of data to be processed (or even the specific information), the purposes of the processing and any special aspects of the processing which may affect the individual.

2.2 Second Principle

2.2.1 The second principle provides that "**personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".**

2.2.2 The second data protection principle prohibits further processing of data in a manner incompatible with the purpose for which the information was obtained. The interpretative provisions for this principle are contained in **Schedule 1, Part II, Paragraph 5**.

2.2.3 The purpose for which the data was obtained can be specified in the notification given to the Information Commissioner's Office, or in terms of notice given to satisfy the first data protection principle set out in **Schedule 1, Part II, Paragraph 2**.

2.2.4 Further processing should not be incompatible with those stated purposes. To assist with that assessment, consideration should be given to the purpose for which the personal data are to be used by the third party, to whom it is to be disclosed.

2.2.5 Unless disclosure to third parties can be considered compatible with the purpose for which the data were obtained the Act effectively prohibits data-sharing. As a general rule of thumb, provided that the purpose is not contradictory to the original purpose it will be considered consistent.

2.2.6 There is no requirement under the 1998 Act to obtain consent for the (proposed) use but the data subject must be informed.

2.3 Third Principle

2.3.1 The third principle provides that **"personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed**".

2.3.2 In order to comply with this principle, data controllers should, as far as possible, identify the minimum amount of information that is required in order to properly fulfil their purpose. This will be a matter of fact and circumstances in each case.

2.3.3 Data controllers should not hold information on the basis that it might possibly be useful in the future, without knowing how that information will be used.

2.3.4 For all data held, the data controller should consider:

- The number of individuals on whom information is held;

- The number of individuals for whom it is used;
- The nature of the personal data;
- The length of time it is held;
- The way it was obtained;
- The possible consequences for individuals of the holding or erasure of the data;
- The way in which it is used; and
- The purposes for which it is held.

2.4 Fourth Principle

2.4.1 The fourth principle provides that "**personal data shall be accurate and, where necessary, kept up to date**".

2.4.2 This principle will not be contravened because of any inaccuracy in personal data where:

(a) Taking account of the purpose or purposes for which the data was obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of that data; **and**
(b) If the data subject has notified the data controller of the data subject's view that the data is inaccurate, the data indicates that fact.

2.5 Fifth Principle

2.5.1 The fifth principle provides that "**personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes**".

2.5.2 Data controllers must ensure that procedures are in place to ensure that personal data is reviewed regularly and information which is no longer required for their purposes is deleted.

2.5.3 The need to review personal data is particularly relevant where the data is held as a result of a relationship between the data controller and the data subject, where that relationship ceases to exist, e.g. where the data subject is an employee who has left the employment of the data controller.

2.6 Sixth Principle

2.6.1 The sixth principle provides that "**personal data shall be processed in accordance with the rights of data subjects under this Ac**t".

2.6.2 A data controller will contravene this principle only if:

(1) S/he fails to supply information pursuant to a Subject Access Request under **section 7** of the 1998 Act; or
(2) S/he fails to comply with notices given under the following provisions of the 1998 Act:
    i) **Section 10** *(right to prevent processing likely to cause damage or distress)*;
    ii) **Section 11** *(right to prevent processing for the purposes of direct marketing)*; or
    iii) **Section 12** *(rights in relation to automatic decision-taking)*; or
(3) S/he fails to comply with a notice given under **section 12A** of the Act *(right to require data controller to rectify, block, erase or destroy inaccurate or incomplete data or cease holding such data in a way incompatible with the data controller's legitimate purpose)* in respect of exempt manual data only during the transition period up to including 23 October 2007.

2.7 Seventh Principle

2.7.1 The seventh principle provides that "**appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data**".

2.8 Eighth Principle

2.8.1 Finally, the eighth principle provides that "**personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data**".

2.9 Consideration of the Data Protection Principles

2.9.1 The Data Protection principles must be interpreted in accordance with **Schedule 1, Part II** of the 1998 Act.

2.9.2 The first and second data protection principles are of particular significance in determining whether data-sharing is lawful. Careful consideration must, therefore, be given to these principles when considering data-sharing and Subject Access Requests.

Chapter 3: Personal Data & Relevant Filing Systems

3.1 Introduction

3.1.1 The terms of the 1998 Act apply only to information which falls within the definition of "personal data". It is essential therefore to identify whether information held is personal data. If the information does not satisfy the definition of personal data then the terms of the 1998 Act do not apply. For example, information about an individual in a professional capacity can often be processed without invoking the terms of the 1998 Act.

3.2 The European Data Protective Directive

3.2.1 Article 2 of the European Data Protective Directive 95/46/EC defines personal data by reference to whether information relates to an identified or identifiable individual.

3.2.2 Article 3 of the Directive provides that the Directive only applies to the processing of personal data where the processing is whole or partly by automatic means or where it is non-automated processing of personal data which forms part of a filing system (as defined by Article 2 (c) of the Directive) or is intended to form part of a filing system.

3.2.3 In effect, therefore, the Directive first considers whether the information relates to an identifiable individual and then describes the two different types of processing which will bring information within the scope of the Directive.

3.2.4 The domestic courts are under a strong obligation to interpret domestic legislation so as to give it a construction which is compatible with European Data Protective Directive[2].

3.3 The Data Protection Act 1998 & Personal Data

3.3.1 The 1998 Act effectively incorporates the definition of personal data contained in the European Directive, setting out that the nature of the processing should first be considered to determine whether the information in question is "data", be it processed by automatic means or non-automated processing within a filing system. Then, the 1998 Act considers whether the "data" is "personal data".

3.3.2 In addition, the 1998 Act introduces two further types of manual processing, which where it relates to an identifiable individual, will involve the processing of personal data. These additional categories of processing concern:

(1) Processing information as part of an "accessible record"; and

[2] *Litster v Forth Dry Dock and Engineering Co Ltd* [1990] 1 AC 546

(2) Processing recorded information held by a public authority.

3.3.3 Accordingly, the 1998 Act considers four types of data which can be referred to as:

(1) Electronic data;
(2) Data forming part of a relevant filing system;
(3) Data forming part of an accessible record (that does not otherwise fall with the above two categories); and
(4) Data recorded by a public authority

3.3.4 Personal data can be **objective** factual information (such as an individual's personal details) or **subjective** information including opinions and any indications of the intention of the data controller.

3.3.5 A reference to an individual's name alone is not in itself "personal data" within the meaning of the 1998 Act, but the particular context in which the name appears may import information about that individual which does fall within the meaning of the Act.

3.3.6 In order to establish whether the data held by the data controller (e.g. COPFS) is "personal data", there are a number of steps that must be followed. You must establish:

(1) That the material is "data" within the definition set out in the 1998 Act;
(2) Whether a living individual can be identified from the data, or, from the data and other information in your possession, or likely to come into your possession; and
(3) Whether the data "relates to" an identifiable living individual

3.3.7 In order, therefore, for material to be "personal data" it must consist of identified or identifiable information within the meaning set out in the 1998 Act and it must relate to an identified or identifiable person, i.e. the material must contain both information and an identifier.

3.4 Data & Relevant Filing Systems

3.4.1 All information stored **electronically** is within the definition of data, for example, databases (e.g. PROMIS, SOS-R, FOS) and the content of email and other electronic documents.

3.4.2 The definition also includes data stored **manually**, provided it is part of a "**relevant filing system**." A statutory definition can be found in **Section 1** of the 1998 Act as detailed in Annex A of this manual. After judicial consideration by the Court of Appeal in England, in ***Durant v Financial Services Authority***[3], a

[3] [2003] EWCA Civ 1746.

relevant filing system was found to mean highly structured files, which are structured either by reference to individuals or by reference to criteria relating to individuals. In effect, therefore, to constitute a relevant filing system, manual files must in particular (a) be structured by reference to individuals or criteria relating to individuals and (b) must be structured in such a way that specific information relating to a particular individual is readily accessible, e.g. a set of files relating to disciplinary matters sorted in alphabetical name order.

3.4.3 The question as to whether a particular manual record or file is part of a relevant filing system is a question of fact and circumstances in every case and files or systems that do not have any clear systematic internal indexing mechanism probably do not fall under the definition.

3.4.4 To constitute a 'system' the contents must contain information about more than one individual. The system may consist of files ordered by topic which are internally structured - through indexing or sub-dividing - to contain information relating to individuals; or the system may consist of several self contained files each relating to one individual which are structured by common categories and contain similar information.

3.4.5 One file containing information about one individual without any similar files forming a set is **not** a relevant filing system (although the file may subsequently become part of a relevant filing system at a later date with the addition of further information).

3.4.6 It must be possible to retrieve information about an individual without the need to leaf through the entire file. Essentially, the search process must be capable of being carried out with the same simplicity as a key-word search on an electronic database.

3.4.7 The standard to establish whether a collection of files or information is a relevant filing system has been referred to as the 'temp test'. The test is whether a temporary employee with a superficial knowledge of the filing system and with no particular knowledge of the employer's business would able to extract specific information about an individual. Where there are external indicators in the structure of the file to assist the temp in locating information about an individual, this will constitute a relevant filing system.

3.4.8 The standard imposed by ***Durant*** is a high one and the Information Commissioner holds the view that few *manual* systems will fall under the 1998 Act.

3.4.9 Where the data controller is a public authority, such as COPFS, the definition of data is broadened by the additional category of **unstructured manual data**[4]. This is a 'catchall' category which applies to any recorded

[4] Section 1(1)(e) of the 1998 Act.

information held by a public authority which is not otherwise captured by the definition of data in **Section 1**. On this broader definition it would appear that all manual files held by public authorities – whether structured or unstructured - are "data" within the terms of the 1998 Act.

3.4.10 The category of unstructured manual data, however, has special exemptions from compliance with certain data protection principles (**Section 33A**) and from compliance with a Subject Access Request (**Section 9A**). The impact is considered in Chapters 5, 6, 9 and 10 of this Manual.

3.5 Identification of a Living Individual

3.5.1 Once you have established that the material held falls within the definition of "data", you must then consider whether a living individual can be identified from the data, or, from the data and other information in your possession, or likely to come into your possession. If a living individual cannot be so identified then that data is not personal data for the purposes of the 1998 Act.

3.5.2 The question considers two levels of identification:

a) Identified from data; or
b) Identified from data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

3.5.3 Establishing whether a living individual can be identified will be relatively straightforward when considering most requests. The data subject must be alive for information about them to be regarded as personal data and attract the protection afforded by the terms of the Act.

3.5.4 An individual is "identified" if you are able to distinguish that individual from other members of a group. In most cases, an individual's name together with some other information (e.g. date of birth) should be sufficient to identify them. Equally, however, the absence of an individual's name does not necessarily mean that the individual cannot be identified.

3.5.5 A data subject is identified if the data controller can distinguish them from other individuals. The information may identify the data subject directly (e.g. by name) or indirectly (e.g. bank account number) or by a combination of pieces of information which identify the group to which the individual belongs (e.g. name and profession).

3.5.6 A data subject may also be identifiable where the data controller is likely to come into possession of further information that will transform 'data' already held into 'personal data'. The likelihood of this eventuality is for the data controller to assess.

3.5.7 The data can relate to the living individual whether it is in relation to the individual's personal or family life, business or profession.

3.5.8 It should be noted that only individuals can be data subjects. Organisations cannot be data subjects.

3.6 Establishing whether the data *relates* to an identifiable living individual

3.6.1 Data is only personal to the extent that it relates to the data subject. In simple terms there must be a connection between the data and the data subject.

3.6.2 Just because an individual's name features in a document does not necessarily mean that the information contained within the document is personal data about the individual. **Not all personal information held by the data controller will constitute personal data.**

3.6.3 The distinction between personal information and personal data will be based on the relevance and proximity of the information to the data subject.

3.6.4 Where the following questions can be satisfied, this will tend to support the view that, the **information does relate to the individual**:

a) The **content** of the information – is it about the data subject? Is the individual the focus of the information? Is the information biographical in the sense that it goes beyond the individual's mere involvement in the incident? Examples might include data about an individual which includes his/her medical history, criminal history record and his/her work record.
b) The **purpose** of the information – is it being used to evaluate or influence the status of the data subject?
c) The **result** of the information – is it likely to have an impact on the data subject's rights and interests?

3.6.5 There may be circumstances where an individual requests information which relates to them in their capacity as an office-bearer of a corporate body or otherwise than in a personal capacity. The circumstances of such a request must be considered carefully to determine whether the information requested is personal data about that individual or whether the information is truly about the body corporate[5]. The 'content' of the information should be considered using the questions detailed above, at paragraph 3.6.4.

3.7 "Anonymised" data

3.7.1 A Data Controller may modify data to remove personal references and render the content anonymous.

[5] For an example see *Terence William Smith v Lloyds TSB Bank Plc,* [2005] EWHC 246 (Ch).

3.7.2 If the data controller is no longer able to single out an individual and treat that individual differently, the data cease to be personal data. This was affirmed by the Inner House of the Court of Session[6] which concluded that a modified and anonymous version of information held was not personal data. [Note: This decision was made in the context of **Section 34** of the Freedom of Information (Scotland) Act 2002 which relies on the definition of personal data in **Section 1** of the 1998 Act.]

3.7.3 The Information Commissioner, however, considers that true anonymisation is difficult to achieve because the data controller will typically retain possession of the original data from which the anonymous data has been produced. Where both versions of the data are held and where they could be reconciled to render the data subject identifiable then both sets of data remain 'personal data'.

3.7.4 Where the data controller does destroy the original data and only has possession of the anonymous data and is unlikely to come into possession of any other information which will render the individual identifiable, they cease to be the data controller of that retained information.

3.8 Sensitive Personal Data (Section 2)

3.8.1 The content of certain data is deemed to be sensitive and attracts a higher degree of privacy. The categories of data are defined by **Section 2** and are personal data consisting of information as to:

a) The racial or ethnic origin of the data subject;
b) His/her political opinions;
c) His/her religious beliefs or other beliefs of a similar nature;
d) Whether s/he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992;
e) His/her physical or mental health or condition;
f) His/her sexual life;
g) The commission or alleged commission by him/her of any offence; or
h) Any proceedings for any offence committed or alleged to have committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

3.8.2 In the context of the work of COPFS, attention is particularly drawn to the last two categories relating to the commission/alleged commission of any offence and any related offences.

3.8.3 In order to comply with the first data protection principle one of the conditions within **Schedule 3** must be satisfied, in addition to satisfying one of

[6] *The Common Services Agency v The Scottish Information Commissioner,* 2007 SLT 7.

the conditions in **Schedule 2**. Further details on these conditions are detailed in Paragraphs 2.1.10 and 2.1.11 of this Manual.

Chapter 4: Rights of the Individual under the Data Protection Act 1998

4.1 Introduction

4.1.1 The 1998 Act gives individuals certain rights in respect of personal data held about them by others. These rights can be separated into 6 main categories:

(1) Rights to subject access;
(2) Right to prevent processing likely to cause damage or distress;
(3) Right to prevent processing for the purposes of direct marketing;
(4) Rights in relation to automated decision taking;
(5) Right to take action for compensation if the individual suffers damage by any contravention of the 1998 Act by the data controller; and
(6) Right to take action to rectify, block, erase or destroy inaccurate data.

4.2 Rights of Subject Access

4.2.1 **Section 7** of the 1998 Act provides that Subject Access is the primary right under the 1998 Act and is the mechanism by which an individual ("data subject") may request and retrieve personal data held by a data controller. The request should contain sufficient information to allow the Data Controller to find the information sought.[7]

4.2.2 It is not an unlimited right of access and the data controller will consider the request in light of their obligations and any applicable exemptions. Where compliance with a Subject Access Request will disclose information relating to a third party the data controller must balance the data subject's rights under the Act with considerations of third party privacy.

4.2.3 The data subject is entitled to be provided with information constituting personal data in an intelligible and permanent form but has **no absolute right to be provided with original or copy documents.** The information provided may be contained in a document prepared for the purpose of responding to the request and/or in the form of copy documents redacted if necessary to remove matters that do not constitute personal data.

4.2.4 The provision of the information should be supplied in permanent form (usually a copy) except where the supply of a copy in permanent form is not possible or would involve a disproportionate effort, or the data subject agrees otherwise.

4.2.5 The 1998 Act does not provide an interpretation of the meaning of "disproportionate effort", and will be a question of fact and circumstance in each individual case. Relevant factors will include the cost of provision of information;

[7] Section 7(3) of the 1998 Act

the length of time that it may take to provide the information; the level of difficulty involved in providing the information; and the size of the organisation to which the request has been made. All such factors, however, must be carefully balanced against the effect on the data subject.

4.2.6 Further guidance in relation to subject access requests are contained in Chapter 12 of this Manual.

4.3 Right to Prevent Processing Likely to Cause Damage or Distress

4.3.1 Under **section 10** of the 1998 Act, a data subject is entitled to serve a written "data subject notice" on data controllers requiring them not to begin or to cease processing personal data relating to them, where such processing is causing or is likely to cause unwarranted substantial damage or distress to them or another.

4.3.2 If a data controller receives a “data subject notice”, s/he must, within 21 days, provide the data subject with a written notice stating either:

(a) That s/he has complied with the data subject notice, or intends to comply with it; or
(b) The extent to which s/he intends to comply with the data subject notice (if at all) and explaining the parts of the data subject notice s/he considers to be unjustified in any way.

4.3.3 If the position is disputed the data subject can apply to the court which will consider the matter and, if satisfied, order the data controller to take such steps as are necessary to comply with the notice.

4.3.4 An individual is only entitled to serve a data subject notice where it relates to personal data in respect of which s/he is the data subject.

4.3.5 An individual is not entitled to serve a data subject notice if any of the first 4 conditions of processing set down in **Schedule 2** of the 1998 Act apply, i.e.:

(1) S/he has given a valid consent to the processing (although consent may be withdrawn);
(2) The processing is necessary for the taking of steps, at the data subject’s request, with a view to entering into a contract, or the processing is necessary for the performance of a contract to which the data subject is a party;
(3) The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract; or
(4) The processing is necessary to protect the individual’s vital interests, (i.e. it is a life and death situation).

4.3.6 The court must decide in each case whether the damage or distress is substantial and unwarranted, but the Information Commissioner takes the view that a data subject notice is only likely to be appropriate where the particular process has caused, or is likely to cause, someone to suffer loss or harm, or upset and anguish of a real nature, over and above annoyance level, and without justification.

4.4 Right to Prevent Processing for Purposes of Direct Marketing

4.4.1 In terms of **Section 11** of the 1998 Act, anyone can ask a data controller not to process information relating to him or her for direct marketing purposes. This should be done by written notice. The data controller must respond to the written notice as soon as practicable. There are no exceptions to this.

4.4.2 The data subject can apply to the court for an order if the data controller fails to comply with the written notice.

4.4.3 "Direct Marketing" is defined in the 1998 Act as meaning the communication, by whatever means, of any advertising or marketing material which is directed to particular individuals.

4.5 Rights in Relation to Automated Decision-Making

4.5.1 **Section 12** of the 1998 Act provides that data subjects can require, by written notice, a data controller to ensure that no decision, which significantly affects them, is based solely on the processing of their personal data by automatic means. Data subjects also have the right to be informed of the logic of any automated decision process taken concerning them.

4.6 Compensation for Failure to Comply with Certain Requirements

4.6.1 **Section 13** of the 1998 Act provides that an individual can claim compensation from a data controller for damage or damage and distress caused by any breach of the 1998 Act. Compensation for distress alone can only be claimed in limited circumstances.

4.6.2 Compensation may only be awarded where the data controller is unable to prove that s/he had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

4.6.3 "Damage" includes both financial loss and physical injury.

4.6.4 Compensation for distress alone may be awarded where the contravention relates to the processing of personal data for "special purposes", i.e. journalistic, artistic or literary purposes.

4.7 Right of Rectification, Blocking, Erasure, Destruction

4.7.1 **Section 14** of the 1998 Act provides that individuals can apply to the court to order a data controller to rectify, block or destroy personal details if they are inaccurate or contain expressions of opinion based on inaccurate information.

4.7.2 Data is considered inaccurate if the data is incorrect or misleading as to any matter of fact.

4.7.3 The court may also order, where reasonably practicable, that the data controller inform any third parties to whom the inaccurate date has been disclosed. In doing so, the court should have regard to the number of persons who would require to be so notified.

4.7.4 If the court finds that the subject has suffered damage or damage and distress as a result of the data controller's processing of inaccurate data, compensation may be awarded.

4.8 Rights of Data Subjects in Relation to Exempt Manual Data

4.8.1 **Section 12A** of the 1998 Act entitles a data subject to give notice in writing to a data controller to require a data controller to rectify, block, erase or destroy data that is inaccurate or incomplete, or to require the data controller to cease holding such data in a way which is incompatible with the legitimate purposes pursued by the data controller. The data subject must state why they think there is an inaccuracy or incompatibility.

4.9 Limitations to the Rights of the Individual to Personal Data

4.9.1 The 1998 Act recognises that there will be limited circumstances in which personal data should not be disclosed. These are contained in **Sections 28-36** of the 1998 Act and are discussed in more detail in Chapters 5, 6 and 9 of this Manual.

Chapter 5: Exemptions – General Principles

5.1 Introduction

5.1.1 The 1998 Act creates various exemptions from compliance with its terms. The effect of an exemption is to permit processing which would otherwise be in breach of the 1998 Act. The exemption may refer to **specific data protection principles, a specific section of the 1998 Act, or to a class exemption** as detailed below.

5.1.2 The 1998 Act imposes duties on data controllers and gives rights to data subjects. **Part IV** of the 1998 Act provides for exemptions both from complying with these duties (non-disclosure provisions) and from applying the rights of the data subject (subject information provisions). These are known as "**class exemptions**". Further information in respect of both of these categories of exemption is contained later in this chapter.

5.1.3 In assessing whether an exemption applies each application must be considered on its own merits. **It will not be appropriate to adopt a blanket policy of applying a particular exemption to all similar requests.**

5.1.4 Each exemption is very specific and contains details of exactly which provisions of the 1998 Act are to be exempt from the processing in question. All other provisions of the 1998 Act continue to apply with full force.

5.1.5 One exemption may be applied to prevent disclosure of personal data to a data subject in response to an SAR, while another exemption may be applied to justify data-sharing with a third party organisation. The terms of the Act are complex and careful consideration must be given to the terms of each exemption before it is applied.

5.2 Non-Disclosure Provisions

5.2.1 The 1998 Act imposes certain duties on data controllers which have the effect of safeguarding personal data and ensuring that data is held and processed appropriately. These are referred to as the "**non-disclosure provisions**" and, in effect, are:

(a) the first data protection principle, except to the extent to which it requires compliance with the conditions in **Schedules 2** and **3** of the Act;
(b) the second, third, fourth and fifth data protection principles; and
(c) **Sections 10** and **14(1)-(3)** of the Act *(right to prevent processing likely to cause damage or distress & rectification, blocking, erasure and destruction of inaccurate data)*

5.2.2 **Exemption from these provisions operates to enable disclosure where this is judged to be in the public interest**.

5.2.3 In order to rely upon an exemption from the non-disclosure provisions, the data controller must satisfy a two stage test:

(1) The data controller (e.g. COPFS) must be satisfied that the disclosure falls within one of the following sections, namely, **Section 29(3)** (the 3rd crime and taxation exemption), **Section 34** (information made available to the public by or under any enactment); or **Section 35** (disclosures required by law or made in connection with legal proceedings); and
(2) If the disclosure falls within one of those sections, the data controller must consider each of the non-disclosure provisions in turn and decide which, if any, would be inconsistent with the disclosure in question. The data controller is then entitled to disapply only those provisions, the application of which would give rise to an inconsistency, and only then to the extent of that consistency.

5.3 Subject Information Provisions

5.3.1 As described in Chapter 4 of this Manual, **Part II** of the 1998 Act gives individuals (data subjects) the right of access to personal data. These rights are referred to as the "**subject information provisions**" and, in effect, are:

(a) The first data protection principle to the extent to which it requires compliance with **paragraph 2** of **Part II** of **Schedule 1**; and
(b) **Section 7** of the 1998 Act.

5.3.2 The scope of each exemption to the subject information provisions is limited and it is the view of the Information Commissioner's Office that where personal data is held by a data controller it will be **virtually impossible to refuse a Subject Access Request entirely**. It is essential, therefore, that the exact terms of any exemption are checked before seeking to rely on the exemption as each exemption is expressed to apply to specific provisions and in specific circumstances only. The meaning and extent of exemptions are not always self-evident or easy to follow and, in cases of doubt, guidance should be sought from the RIU.

5.4 Partial Exemptions: Right of Access to Personal Data

5.4.1 **Section 7(4)** of the 1998 Act provides a **quasi-exemption which details that a data controller is not obliged to comply with a Subject Access Request where this would disclose third party information**. As with all exemptions this provision should be exercised cautiously and as much information as possible must be provided. This may be achieved by: editing references to third parties; by seeking consent to disclose; or disclosing in the

absence of consent, where appropriate. Further guidance on disclosure of third party information is contained in Chapter 9 of this Manual.

Chapter 6: Categories of Exemptions

6.1 Introduction

6.1.1 The primary exemptions set down in **Part IV** of the 1998 Act concern:

- Safeguarding national security;
- Prevention or detection of crime;
- Apprehension or prosecution of offenders;
- Assessment or collection of tax or duty;
- Personal data concerning physical or mental health;
- Personal data concerning school pupils;
- Personal data processed by government departments or local authorities for the purposes of social work;
- Regulatory functions exercised by public "watchdogs";
- Journalistic, literary or artistic purposes;
- Research, historical and statistical purposes;
- Where the information is obliged to made under enactment;
- Where disclosure is required by law;
- Where disclosure is necessary in connection with legal proceedings;
- Where data is processed only for personal or family affairs;
- Where data is processed for the purpose of conferring by the Crown of any honour; and
- Where a claim to legal professional privilege could be maintained.

6.2 National Security (Section 28 of the 1998 Act)

6.2.1 This exemption is applicable if necessary for the purposes of safeguarding national security and provides an exemption from any of the provisions of:

(a) the data protection principles,
(b) Parts II *(rights of data subjects)*, III *(notification by data controllers)* and V *(enforcement)*; and
(c) **Section 55** *(unlawful obtaining etc. of personal data)* of the 1998 Act

6.2.2 Thus, **the exemption is from all of the data protection principles** (including both the non-disclosure and the subject information provisions). In effect, therefore, this exemption could be applied both to justify data-sharing with a third party organisation and to prevent disclosure of personal data to a data subject in response to a Subject Access Request.

6.2.3 A certificate signed by the Lord Advocate (as a Minister of the Crown) that the exemption is required is conclusive of that fact.

6.3 Crime and Taxation (Section 29 of the 1998 Act)

6.3.1 This exemption is available where personal data is processed for the purposes of:

(1) the prevention of detection of crime,
(2) the apprehension or prosecution of offenders, or
(3) the assessment or collection of any tax or duty or of any imposition of a similar nature

6.3.2 Processing for these purposes is **exempt from the first data protection principle** (exempt to the extent to which it requires compliance with the conditions in **Schedule 2** and **3**) and **Section 7** in any case to which the application of those provisions would be likely to prejudice any of the matters mentioned in **Section 29**.

6.3.3 **Section 29(2)** provides that personal data is exempt from the subject information provisions to the same extent as personal data processed for any of the purposes mentioned in **paragraph 6.3.1** above where it is personal data which:

(a) Is processed for the purposes of discharging statutory functions; and
(b) Consist of information obtained for such a purpose from a person who had it in his/her possession for any of the purposes referred to at **paragraph 6.3.1** above.

6.3.4 **Section 29(3)** provides that personal data is exempt from the non-disclosure provisions in any case in which:

(a) The disclosure is for any of the purposes mentioned in **paragraph 6.3.1**, and
(b) The application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that paragraph.

6.4 Health, Education and Social Work (Section 30 of the 1998 Act)

6.4.1 This provides for the Lord Chancellor to make orders providing exemptions from the subject information provisions in relation to health, education and social work records.

6.5 Regulatory Activity (Section 31 of the 1998 Act)

6.5.1 This section provides for exemption from the subject information provisions for personal data processed for the purposes of discharging a wide range of regulatory functions.

6.6 Journalism, Literature and Art (Section 32 of the 1998 Act)

6.6.1 **Section 32** provides for particular exemptions (from the data protection principles *(except the seventh data protection principle)*, **Section 7**, **Section 10**, **Section 12**, **Section12A** and **Section 14(1) & (3)**) where processing is with a view to publication by any person of any journalistic, literary or artistic material, and where the data controller believes that publication would be in the public interest.

6.7 Research, History and Statistics (Section 33 of the 1998 Act)

6.7.1 This section provides for exemption from **Section 7** provided the following relevant conditions are met:

1) That the data are not processed to support measures or decisions with respect to particular individuals; and
2) That the data are not processed in such a way that substantial damage or distress is, or is likely to be, caused to any data subject.

In addition, the results of the research or any resulting statistics are not made available in a form which identifies data subjects.

6.7.2 Where the conditions are satisfied the processing will not be regarded as incompatible with the second data protection principle; and data can be kept indefinitely, notwithstanding the terms of the fifth data protection principle.

6.7.3 "Research purposes" includes statistical and historical purposes.

6.7.4 **Section 33(5)** provides that personal data should not be treated as processed otherwise than for research purposes merely because the data is disclosed:

(a) To any person, for research purposes,
(b) To the data subject or a person acting on his/her behalf,
(c) At the request, or with the consent, of the data subject or a person acting on his/her behalf; or
(d) In circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within **paragraphs (a), (b)** or **(c)** above.

6.8 Manual Data Held by Public Authorities (Section 33A of the 1998 Act)

6.8.1 This exemption applies to the category of 'unstructured manual data' held by public authorities in terms of **Section 1(1)(e)**.

6.8.2 Data held in this format is exempt from:

(a) The first, second, third, fifth, seventh and eighth data protection principles;
(b) The sixth principle except so far as it relates to rights conferred on data subjects by **Sections 7** and **14**;
(c) **Sections 10** to **12** *(right to prevent processing likely to cause damage or distress; right to prevent processing for purposes of direct marketing; and the rights in relation to automated decision-taking)*;
(d) **Section 13** *(compensation for failure to comply with certain requirements)*, except so far as it relates to damage caused by a contravention of **Section 7** or of the fourth data protection principle and to any distress which is also suffered by reason of that contravention;
(e) **Part III** *(notifications by data controllers)*; and
(f) **Section 55** *(unlawful obtaining etc. of personal data)*.

6.9 Information Available to the Public by or under Enactment (Section 34 of the 1998 Act)

6.9.1 Personal data which the data controller is obliged to make available to the public under enactment are exempt from:

(a) The non-disclosure provisions;
(b) The subject information provisions; and
(c) The fourth data protection principle and **Section 14(1)** to **(3)**.

6.10 Disclosures required by law or made in connection with legal proceedings etc (Section 35 of the 1998 Act)

610.1 This section provides for exemption from the non-disclosure provisions where disclosure is required by or under any enactment, by any rule of law or by the order of a court (**Section 35(1)**) or in connection with legal proceedings (including prospective legal proceedings) or for the purpose of obtaining legal advice (**Section 35(2)**), or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

6.11 Parliamentary Privilege (Section 35A of the 1998 Act)

6.11.1 This exemption applies where it is required for the purpose of avoiding an infringement of the privileges of either House of Parliament and provides for exemption from:

(a) the first data protection principle (except to the extent required by **Schedule 2** and **3**);
(b) the second to fifth data protection principles;
(c) **Section 7**; and
(d) **Sections 10** and **14(1) & (3)** of the 1998 Act.

6.12 Domestic Purposes (Section 36 of the 1998 Act)

6.12.1 Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes) are exempt from the data protection principles and the provisions of **Parts II** and **III**.

6.13 Miscellaneous Exemptions (Section 37 of the 1998 Act)

6.13.1 **Section 37** & **Schedule 7** of the 1998 provide for further miscellaneous exemptions from the subject information provisions:

a) ***Armed Forces*** - provides an exemption to protect the combat effectiveness of the armed forces.
b) ***Judicial Appointments and Honours*** – provides an exemption for personal data processed for the purposes of making appointments of judges and QCs, and the conferring of honours or dignities.
c) ***Crown Employment and Crown or Ministerial Appointments*** - provides a power for the Lord Chancellor to make orders providing exemptions in relation to crown appointments. An order designating a limited number of appointments has been made.
d) ***Management forecasts etc****.* – provides an exemption for personal data processed for the purposes of management forecasting or management planning.
e) ***Corporate finance*** - provides an exemption for personal data processed for corporate finance services
f) ***Negotiations*** – provides an exemption for personal data consisting of records of the data controller's intentions in relation to negotiations with the data subject.
g) ***Examination marks*** - modifies the 40 day maximum period for dealing with subject access requests in relation to examination marks.
h) ***Client confidentiality (legal privilege)*** – provides an exemption for personal data in respect of which legal professional privilege could be claimed and has also been applied to legal advice given by departments' in-house lawyers.
i) ***Self-incrimination*** - provides an exemption for circumstances in which by granting access a person would incriminate himself in respect of an offence other than one under the 1998 Act.

6.13.2 In addition, **Section 37** & **Schedule 7** of the 1998 provide for further miscellaneous exemptions from **Section 7** of the 1998 Act:

(a) ***Confidential references given by the data controller*** –provides an exemption for personal data relating to confidential references given by

data controllers in relation to education, employment or the provision of services; and

(b) ***Examination scripts etc***. – provides an exemption for personal data relating to examination scripts, consisting of information recorded by candidates during an academic, professional or other examination.

6.14 Powers to make further exemptions by order

6.14.1 **Section 38** provides a power for the Lord Chancellor to make orders providing exemptions where disclosure of information is statutorily prohibited or restricted, subject to certain conditions.

Chapter 7: Freedom of Information (Scotland) Act 2002 & the Environmental Information Regulations

7.1 Introduction

7.1.1 The Freedom of Information (Scotland) Act 2002 (FOISA) and Environmental Information Regulations (EIR) also regulate requests for information. Requests may be covered by more than one regime and it is important to recognise this and respond appropriately.

7.1.2 From 1 January 2005 everyone has a right of access to the information held by public authorities. Some information is exempt, such as material that might endanger national security, or information which is already published (which is described in the authority's Publication Scheme), and some information will fall instead under the 1998 Act or Environmental Information Regulations.

7.1.3 Information requests concerning the environment are governed by Environmental Information Regulations. **'Environmental information'** covers a broad spectrum of issues - not only the obvious subjects such as pollution and conservation, but also the built environment such as developments, planning, and anything affecting health.

7.2 Comparative Rights under the Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002

7.2.1 If an individual makes a Subject Access Request under data protection, the request is **exempt** from FOI. Similarly, if the individual makes no reference to either legislation in his/her request but is clearly seeking information about him/herself, it should be handled under data protection and will, again, be **exempt** from FOI.

7.2.2 If the request is for information about another living individual, the request will fall under FOI but certain data protection considerations will still apply. In particular, disclosure must **not** breach the data protection principles or cause the release of sensitive personal data which may lead to damage or distress to the individual.

7.2.3 If the request is for information which contains incidental references to living people, any disclosure should not be in breach of the data protection principles.

7.2.4 Annex D contains further details of the comparative rights of access under the Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002.

Chapter 8: The Role of the Information Commissioner

8.1 Introduction

8.1.1 The Information Commissioner[8] oversees the operation of the Data Protection Act 1998 throughout the UK. The Commissioner has responsibility for:

a) Promoting the following of good practice and observance of the Act by data controllers; and
b) Disseminating information about the Act.

8.1.2 'Good practice' is defined as such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, and includes (but is not limited to) compliance with the requirements of this Act.

8.2 Register of Notifications (Section 19)

8.2.1 The Commissioner is required to maintain a register of persons who have given notification under **Section 18** of the Act. Data controllers who wish to be included in this register must specify their "registrable particulars" and provide a general description of measures to be taken for the purpose of complying with the **seventh** data protection principle.

8.2.2 The "registrable particulars" include:

a) The name and address of the data controller;
b) A description of the personal data being or to be processed; and
c) A description of the purpose or purposes for which the data are being or are to be processed.

8.3 Enforcement and non-compliance

8.3.1 The Information Commissioner has responsibility to enforce the provisions of the Act and has extensive powers to investigate alleged breaches and require certain action to be taken.

8.3.2 The Commissioner's investigatory powers are contained within **Schedule 9** of the Act and can extend to powers of entry and inspection and grant of a warrant.

8.3.3 The Commissioner has the following powers to investigate alleged breaches of the Act:

[8] Section 6 - formerly known as the *Data Protection Commissioner* – amended by Freedom of Information Act 2000, Schedule 2 (I), Para 13 (2)

a) Information Notices (**Section 43**);
b) Enforcement Notices (**Section 40**); and
c) **Section 42** Assessments

8.3.4 If the Commissioner receives a request for a **Section 42** assessment or reasonably requires any information for the purposes of determining whether a data controller has complied or is complying with the data protection principles, s/he may serve an **Information Notice** under the authority of **Section 43** requiring the data controller to supply specified information relating to the processing activities.

8.3.5 The Commissioner can issue an **Enforcement Notice** (**Section 40**) where s/he is satisfied that any of the data protection principles are being contravened. This notice can specify the steps that the data controller is required to take or can require the controller to refrain from processing personal data in a particular manner, in order to comply with the Act.

8.3.6 An enforcement notice must contain a statement of the data protection principles which the Commissioner considers have been/are being contravened and his or her reasons for reaching that conclusion.

8.3.7 The enforcement notice must also detail the rights of appeal, as a person on whom an enforcement notice is served may appeal to the Information Tribunal.

8.3.8 An individual who is dissatisfied with the way a data controller has processed information or responded to a Subject Access Request (SAR) can request the Commissioner to carry out an assessment of whether the particular processing was in compliance with the Act, under **Section 42**. The Commissioner must notify the data subject of any assessment and any view formed or action taken as a result.

8.4 Taking a Case to Court

8.4.1 When a data subject is not satisfied with the way their SAR has been handled the complaint can be pursued through the Information Commissioner's Office or as a civil action in the Sheriff Court. Where a civil action is instigated, the data subject may be awarded compensation where they have suffered damage, or distress and damage as a result of any contraventions of the Act by the data controller.

PART B: APPLYING THE DATA PROTECTION ACT WITHIN COPFS

Chapter 9: Applying Exemptions to the Subject Information Provisions

9.1 Introduction

9.1.1 The business of COPFS is likely to invoke a limited number of exemptions:

(1) Section 7(4) of the 1998 Act
(2) Crime & taxation (**section 29**)
(3) Client confidentiality (**Schedule 7**, **paragraph 10**)

Further guidance in respect of each of these exemptions is detailed in the remainder of this chapter.

9.1.2 The above list is not exhaustive and, in some circumstances, other exemptions may apply.

9.2 Information relating to another Individual - Section 7(4)

9.2.1 **Section 7(4)** of the 1998 Act provides that where a data controller cannot comply with a subject access request without disclosing information relating to another individual who can be identified from that information, then s/he is not obliged to comply with the request unless:

(a) The other individual has consented to the disclosure of the information to the person making the request, or
(b) It is reasonable in all the circumstances to comply with the request without the consent of the other individual.

9.2.2 This is not strictly an exemption but it can be invoked in specific circumstances to prevent disclosure of third party information. **This is likely to be relied upon to justify not disclosing police reports and witness statements which may contain a large amount of personal data belonging to another individual.** The scope of **section 7(4)**, however, is limited and as much information as possible should be disclosed – it may, for example, be appropriate to disclose a summary of the contents of the police report, by redacting or editing all third party personal data.

9.3 Crime & Taxation – Section 29

General Principles

9.3.1 The most significant exemption for COPFS is contained within **Section 29** (1) which states that **personal data processed for the purposes of:**

a) **the prevention or detection of crime; or**
b) **the apprehension or prosecution of offenders**

is exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in **Schedule 2** and **3**) and **Section 7** (the Subject Access provision) in any case to which the application of those provisions would be likely to prejudice any of the matters mentioned in **Section 29(1)**.

9.3.2 The terms of the **Section 29(1)** exemption **only** apply where **prejudice is likely** and it will not be appropriate to adopt a blanket approach to the application of the exemption.[9] The data controller needs to make a judgement as to whether prejudice is likely in the circumstances of each case. **There should be a significant chance of prejudice rather than a mere risk.**

9.3.3 This provision can only be relied upon to the extent necessary to avoid the likely prejudice. So where only some of the personal data would be likely to prejudice the purposes within **Section 29(1)**, only that personal data should be withheld and the remainder disclosed (subject to the terms of the 1998 Act). **It is not appropriate to use the exemption to withhold all personal data held where only some would cause prejudice.**

Application of s29 where the case has concluded

9.3.4 As an exemption, **Section 29** of the 1998 Act should be construed narrowly, however, the wording of **Section 29** is wide enough to cover a situation where disclosure of data would not prejudice the apprehension or prosecution of offenders in the particular case to which the data relates but would be likely to prejudice the apprehension or prosecution of offenders in other cases.

9.3.5 This issue was looked at briefly in ***R v The Secretary of State for the Home Department 2003***[10], which considered a highly subjective reporting process which had a direct effect on the *future* status of *individual* Category A prisoners. In its opinion the court held that *"although section 29(1) requires that the issue of whether the disclosure is likely to prejudice the prevention or detection of crime has to be determined in relation to the particular and individual case and once the case in which the disclosure is being sought, this does not mean that one can simply ignore the consequential effect that disclosure in the particular case may have in others".*

[9] The corresponding provision of the 1984 Act was considered by the Information Tribunal: *Equifax Europe Limited v The Data Protection Registrar* (DA/90/25/49/7) and approved by *R (on the application of Lord) v Secretary of State for the Home Department***,** [2003] EWHC 2073.
[10] WL 22002266

9.3.6 The Court further held that when considering Subject Access Requests under **Section 7** of the 1998 Act and the application of the **Section 29** exemption, the key question is whether compliance with **Section 7** *"would be likely"* to prejudice either the prevention or detection of crime or the apprehension or prosecution of offenders and this is a question of fact to be decided in the light of all the circumstances of the case.

9.3.7 It is also worthy of note that the **Section 34** exemption of the Freedom of Information (Scotland) Act 2002, relating to information held by a Scottish public authority for the purposes of investigation and prosecution of crime, applies where the information has been held for that purpose *"at any time".*

9.3.8 The Encyclopaedia of Data Protection states that *"the exemption will cover both the investigation of a crime which has already been committed and the activities of crime prevention and detection. It will apply where a person is suspected of committing an offence and is being investigated, or where a crime has been committed and no one person is suspected. The fact that the police investigation does not result in police action being taken is irrelevant to the application of the exemption*[11]*.* The fact that the exemption can apply even when no action is taken arguably supports the position that this exemption can apply even after an investigation and/or a prosecution has concluded.

9.3.9 On the basis of the above, therefore, the **Section 29** exemption *may* apply even after the case has concluded on the basis that disclosure of the information may jeopardise future prosecutions, e.g. where the material relates to communications between the Crown and the police. **Each Subject Access Request must be decided based on the facts and circumstances of each individual request**.

9.4 Client Confidentiality – Schedule 7, paragraph 10

9.4.1 A further available exemption relates to confidential communication connected with legal proceedings which is exempt from the Subject Information Provisions. **This exemption may be applied to prevent disclosure of certain correspondence which involves candid legal assessment of the case, for example the precognition report or a report by Crown Counsel.**

[11] Paragraph 2-300/3, notes

Chapter 10: Data Sharing of Personal Data & Applying the Exemptions

10.1 Introduction

10.1.1 Organisations or other public bodies frequently request personal information relating to a third party. The 1998 Act does **not** contain a positive legal obligation to provide information to a third party; equally the Act does not expressly prohibit data sharing with a third party. **What the Act does is insist that all processing of personal data, including disclosure, complies with the data protection principles**.

10.1.2 Compliance with the data protection principles may be achieved either because the disclosure complies with the principles or because an exemption operates to disapply the exemptions for the purposes of that processing.

10.1.3 Routine data-sharing and regular requests for information that are the core business of COPFS are likely to invoke a limited number of exemptions. The following guidance should be considered in conjunction with Chapter 17 of the Book of Regulations and the Freedom of Information Guidance Manual.

10.2 Disclosure of Evidence in Criminal Proceedings

Disclosure by the Crown

10.2.1 In order to comply with its disclosure obligations (in the context of criminal proceedings), COPFS has adopted a more proactive approach to the disclosure of evidence.

10.2.3 The Crown's Principles of Disclosure, the Summary of the Crown's Approach to Disclosure and the Disclosure Manual provide full guidance to staff on the disclosure of evidence in criminal proceedings. The overarching disclosure duty on the Crown is set out in ***McLeod v HMA***[12] and was most recently expressed in ***McDonald v HMA***[13].

10.2.4 The disclosure practice was recently scrutinised by the Information Commissioner's Office who were satisfied that the policy is operating in compliance with the 1998 Act.

10.2.5 The requirements of the first data protection principle can be satisfied as follows:

(1) **Schedule 2, Paragraph 6**:

The processing is necessary for the purposes of ***legitimate interests***

[12] (No. 2) 1998 JC 67
[13] 2008 SCCR 154

pursued by the data controller or by the third party or parties to whom the data are disclosed, *except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.*

(2) **Schedule 3, Paragraph 6** (for "sensitive data"):

The processing –

(a) is necessary for the purpose of, or in connection with, ***any legal proceedings*** *(including prospective legal proceedings),*

(b) is necessary for the ***purpose of obtaining legal advice****, or*

(c) *is otherwise necessary for the* ***purposes of establishing, exercising or defending legal rights.***

(3) The disclosure is made solely for the purpose of assisting the proper presentation and preparation of the accused's defence in the context of that criminal prosecution and so is consistent with the purpose for which the information was obtained. The disclosure is made on the understanding that it will be properly handled in accordance with the terms of Article 11 of the Law Society Code of Conduct for Criminal Work.

10.2.6 Where an accused is unrepresented a redacted version of the information may be disclosed rather than a full set of copy documents. Alternatively, the accused may be given access to the information.

Disclosure to the Accused's Representative

10.2.7 The Data Protection Act is primarily concerned with who controls information rather than who owns it. In terms of **Section 1(1)** of the Act, a data controller is *"a person who (either alone or jointly in common with other persons) determines the purposes for which and the manner in which any personal data are…processed".* Thus, the accused's representatives are also "data controllers" of any information that the COPFS provide to them in order to satisfy its disclosure obligations.

10.2.8 Accordingly, solicitors are required to register as data controllers with the Information Commissioner and a failure to do so can result in prosecution and the imposition of fines. It is worth noting that the Information Commissioner actively enforces this requirement and carries out regular checks on solicitors to ensure that they are properly registered.

10.2.9 As a result of their status as data controllers, should a solicitor breach the seventh data protection principle (which places an obligation on data controllers to take all reasonable steps to keep data secure), e.g. through the loss of any of the material disclosed to them by the Crown, then the solicitor could be liable for a breach of the Data Protection Act. Furthermore, a data controller can be held

responsible for the acts of his/her employees and of independent contractors who process data on their behalf[14].

10.3 Witness Service

10.3.1 COPFS routinely share information with the Witness Service, who use that information to assist those witnesses who, for example, require a court familiarisation visit.

10.3.2 The sharing of this information between COPFS and Witness Service must be within the terms of the 1998 Act and in compliance with the data protection principles, and in particular the first and second principles.

10.3.3 COPFS must therefore advise the data subject of the intended use of their data and in this case that their details are being or have been passed onto the Witness Service. **COPFS has chosen to fulfil this obligation by operating an opt-out scheme whereby all witnesses are notified that their details will be passed onto Witness Service on or after a specified date unless they opt-out.**

10.4 Disclosure to the Scottish Children's Reporter Administration

10.4.1 **Section 53** of the **Children (Scotland) Act 1995** provides a statutory framework for the provision of evidence by COPFS to the Scottish Children's Report Administration. In particular, **Section 53(4)** provides that:

> *(4) Where an application has been made to the sheriff—*
>
> *(a) by the Principal Reporter in accordance with a direction given by a children's hearing under section 65(7) or (9) of this Act; or*
>
> *(b) by any person entitled to make an application under section 84 of this Act,*
>
> *the Principal Reporter may request any prosecutor to supply him with any evidence lawfully obtained in the course of, and held by the prosecutor in connection with, the investigation of a crime or suspected crime, being evidence which may assist the sheriff in determining the application; and, subject to subsection (5) below, it shall be the duty of the prosecutor to comply with such a request.*

10.4.2 A Joint Protocol for the Provision of Evidence by the Prosecutor to the Principal Reporter has been agreed providing rules and guidance on the practical application of Section 53(4), (5) and (6) and related situations. This is available at Annex 4A of Chapter 16 of the Book of Regulations.

[14] Data Protection Act 1998, Schedule 1 Part 2, paragraph 10 and 11.

10.4.3 Further guidance on the sharing of evidence between the prosecutor and the SCRA can also be found in Chapter 16 of the Book of Regulations and Annex 4.

10.4.4 When in doubt on the application of the protocol guidance can be sought from Policy Division.

10.5 Disclosure of Information to other bodies for Research

10.5.1 **Section 33** provides an exemption for processing personal data for the purposes of research, history and statistics where the following *"relevant conditions"* are satisfied:

(a) That the data are not processed to support measures or decisions with respect to particular individuals; and
(b) That the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

10.5.2 The section further provides that where the exemption applies:

(a) The further processing of personal data will not be considered incompatible with the purposes for which they were obtained (and will therefore not contravene the second data protection principle);
(b) Personal data is be kept indefinitely, notwithstanding the fifth data protection principle;
(c) Personal data is exempt from Subject Access Rights, provided individuals cannot be readily identified from the resulting research.

10.5.3 **In order to comply with the first data protection principle, which demands "fair and lawful" processing, the data subject should be informed of the intended use of the data.** In determining for the purposes of the first principle whether data is processed fairly or lawfully regard must be had to the method by which they are obtained including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are processed.

10.5.4 Also data is not to be treated as processed fairly unless the data controller ensures as far as practicable that the data subject has, is provided with, or has made readily available to him/her the following information:

(a) The identity of the data controller;
(b) The purpose or purposes for which the data is intended to be processed; and

(c) Any further information which is necessary having regard to the specific circumstances in which the data is or are to be processed, to enable processing in respect of the data subject to be fair.

10.5.5 Therefore to provide information for research purposes and comply with the processing of data in accordance with the first principle, the data controller must notify the data subject that the data may be provided for research purposes or inform the subject as soon as practicable after disclosure.

10.5.6 As it is unlikely that any persons identified in police reports (and accordingly who may be regarded as “data subjects”) will have been previously advised that the information that they provided would be disclosed to a third party for research purposes they would need to be told of the purpose for which the data is intended to be processed at the time that the further disclosure was being considered.

10.5.7 The 1998 Act does not place a requirement on the data controller to obtain the data subject’s consent for such disclosure, just that the subject must be advised that it is to take place. Presumably this will allow the subject if s/he feels it necessary, to ensure the accuracy of any data held by seeking access to the data under **Section 7** of the 1998 Act.

10.5.8 Where data has been stripped of all identifying features before being handed to the researcher it ceases to be personal data and the terms of the Act do not apply.

Chapter 11: Requests for Data-Sharing

11.1 Communication with MPs/MSPs

11.1.1 Where elected representatives seek information on behalf of a constituent the request can be handled within the terms of the **Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002**.[15] The Order was introduced in response to concerns that data controllers would be reluctant to disclose information without the direct consent of the constituent. The Order can be applied where the request is for "sensitive data" (as defined by **Section 2** of the 1998 Act). The Order permits data controllers to release information where all other conditions are satisfied. It does not compel the data controller to disclose personal data.

11.1.2 Where the information requested is non-sensitive, the terms of the Order do not apply. However, the advice of the Information Commissioner is that the data controller may proceed on the assumption that the constituent has consented (which satisfies **Schedule 2, Paragraph 1**) thereby ensures processing in accordance with the first data protection principle.

11.2 Requests from Police Authorities

11.2.1 A police force from another jurisdiction, typically England and Wales, may make a request for information about a particular individual or case.

11.2.2 **Processing in terms of Section 35(2) is exempt from the non-disclosure provisions where disclosure is necessary in connection with legal proceedings.** The data controller may or may not be in a position to judge the necessity of the disclosure and is not obliged to disclose any information in response to the request. The applicant may in those circumstances seek an order of court in order to obtain the information sought.

11.2.3 **Section 29(3)** also provides for exemption from the non-disclosure provisions where disclosure is made for any of the purposes defined in Section 29(1) which includes the prevention or detection of crime and the apprehension or prosecution of offenders. The application of this exemption is subject to the requirement that refusal to disclose the information requested would **prejudice** those purposes. It is for the data controller to judge whether refusal to provide the information is likely to prejudice proceedings and one consideration may be whether the information could be obtained from another source, for example the police force who investigated the offence.

11.2.4 As discussed, the non-disclosure provisions include exemption from the first data protection principle but the terms of Schedule 2 (and Schedule 3, where appropriate) must be satisfied.

[15] SI 2002 No. 2905

11.2.5 In summary, where a police authority requests information about an individual either of the exemptions contained in **Section 35(2)** or **Section 29(3)** *could* be relied upon to justify the disclosure of personal data held about that individual where disclosure is either **necessary** (in terms of **Section 35(2)**) or would **avoid likely prejudice** (in terms of **Section 29(3)**).

11.2.6 The data controller must assess, on the basis of the individual facts and circumstances of each case, whether the disclosure is necessary and whether such disclosure would avoid likely prejudice. The data controller must be able to justify the disclosure.

11.2.7 It may be more difficult to justify sharing information about third parties who are not the subject of legal proceedings or criminal investigation, for example a witness. There would have to be compelling reasons to justify why the disclosure would be necessary in connection with legal proceedings or to avoid prejudice in connection with the prevention or detection of crime.

11.3 Requests for Information for the Purposes of Risk Assessment

11.3.1 Guidance on disclosure of information for the purposes of risk assessment is contained in paragraph 17.31 of the Book of Regulations.

11.4 Requests from Social Work Departments

11.4.1 As a criminal justice partner, social work departments throughout the UK often seek information from prosecuting authorities. Information relating to previous convictions and the nature of particular incidents are likely to be of interest to them.

11.4.2 Where a social work department requests information about an individual either of the exemptions contained in **Section 29(3)** or **Section 35(2)** could be relied upon to justify the disclosure of personal data held about that individual where disclosure is either necessary (in terms of **Section 35(2)** or would avoid likely prejudice (in terms of **Section 29(3)**).

11.4.3 It may be appropriate to give social work departments, *on request*, copies of complaints or indictments (both documents should already be in the public domain in any event). Copies of petitions should not usually be provided, but there is no objection to sharing the general nature of the charge.

11.4.4 Where the accused is a child, or in any other case where the court can reasonably be expected to call for a social enquiry report, it would usually be appropriate to inform the social work department in advance of the time and place of the court hearing.

11.4.5 Should a social work department request any further information, the data controller should assess, on the basis of the individual facts and circumstances of each case, whether the disclosure is necessary and whether such disclosure would avoid likely prejudice. The data controller must be able to justify the disclosure.

11.5 Criminal Injuries Compensation Authority (CICA)

11.5.1 There is guidance in Chapter 17 of the Book of Regulations which indicates that there is a general willingness to provide information, but that provision must be in accordance with duties of confidentiality and legal obligations in terms of the 1998 Act and the ECHR.

11.5.2 In accordance with the guidance already provided an SAR can only be made by the data subject. Where, for example, a relative of a deceased person seeks information in terms of the 1998 Act the request must be denied under those provisions. However, information in the hands of CICA will frequently be a matter of public record, having been discussed in open court and accordingly can frequently be released to a family member as a general request.

11.6 Requests for Information Relating to Civil Proceedings

11.6.1 Often a case has exhausted the criminal justice system and one of the parties involved is now pursuing a civil remedy. The solicitor acting for that party may seek information held by the Procurator Fiscal's Office. There is fuller guidance within Chapter 17 of the Book of Regulations.

11.7 Disclosure of Information to the General Medical Council

11.7.1 The **Medical Act 1983 (Amendment) Order 2000** inserts a new **Section 35A** to the **Medical Act 1983**. The Order came into force on 3 August 2000.

11.7.2 **Section 35A** of the 1983 Act states:

> (1) *For the purposes of assisting the General Council or any of their committees in carrying out functions in respect of professional conduct, professional performance or fitness to practise, a person authorised by the Council may require –*
>
> (a) *A practitioner (except the practitioner in respect of whom the information or document is sought); or*
>
> (b) *Any other person*
>
> *Who in his/her opinion is able to supply information or produce any document which appears relevant to the discharge of any such function, to supply such information or produce such a document*
>
> (2) …
>
> (3) …

(4) *Nothing in this section shall require or permit any disclosure of information which is prohibited by or under any other enactment*

(5) *But where information is held in a form in which the prohibition operates because the information is capable of identifying an individual, the person referred to in subsection (1) above may, in exercising his/her functions under that subsection, require that the information be put into a form which is not capable of identifying that individual*

(5A) In determining for the purposes of subsection (4) above whether a disclosure is not prohibited, by reason of being a disclosure of personal data which is exempt from the non-disclosure provisions of the Data Protection Act 1998 by virtue of section 35(1) of that Act, it shall be assumed that the disclosure is required by this section

(6) *Subsection (1) above does not apply in relation to the supplying of information or the production of a document which a person could not be compelled to supply or produce in civil proceedings before the relevant court (within the meaning of section 38).*

11.7.3 On the basis of this legislation, the GMC can now require the Crown to produce documentation relevant to the regulation of professional conduct. However, documents such as the police report and precognitions may be exempt in terms of **section 35A (6)** as the Crown may not be compelled to produce these in civil proceedings[16].

11.7.4 The Fitness to Practise Directorate of the General Medical Council has indicated that there is no formal paperwork served on havers of documents. The request under **Section 35A** of the 1983 Act is simply made in a letter.

11.7.5 Disclosure to the GMC of documents ingathered in the course of a criminal enquiry, with the exception of the police report and witness precognitions, would not contravene the provisions of the Data Protection Act 1998 as there is a statutory mechanism authorising disclosure.

11.7.6 Such material is sensitive personal data (under **Section 2** of the 1998 Act) as it will undoubtedly relate to the alleged commission of a crime by a named accused person. It is necessary therefore to satisfy the requirements of both **Schedules 2** and **3** to 1998 Act before such disclosure can be made.

11.7.7 **Paragraph 6** of **Schedule 2** allows for processing (including disclosure) if it is necessary for the purposes of legitimate interests pursued by third parties to whom the data is disclosed and **paragraph 7** of **Schedule 3** allows for processing if it is necessary for the exercise of any functions conferred on any person by or under an enactment.

[16] See *McKie v Western Scotland Motor Traction Company* 1952 SC 206; *Ward v HMA* 1993 SLT 1202

11.7.8 Under **Section 34** of the Data Protection Act 1998 personal data is exempt from the non-disclosure provisions where the disclosure is required by or under any enactment. Therefore it will be not be necessary for the Crown to advise an accused medical practitioner that information is being disclosed to the GMC or the purpose of the disclosure.

11.7.9 There is further guidance on dealing with such requests within Chapter 17 of the Book of Regulations. Where Crown Counsel's instructions are required, staff should refer to the Guidance Note on dealing with Chapter 17 requests for information.

11.8 Disclosure of information to the General Teaching Council for Scotland (GTCS)

11.8.1 Under the Teaching Council (Scotland) Act 1965 (as amended) the GTCS has a statutory duty to maintain a register of those entitled to teach in public sector schools and Scotland's Colleges, and to investigate misconduct and consider whether or not, in the light of misconduct, if proved, a person remains a suitable and proper person to be registered as a teacher.

11.8.2 These regulatory functions involve the consideration of complaints and policy issues and the provision of advice and information. Typical activities undertaken will be investigation of complaints, mediation between complainant and respondent, consideration of formal enforcement action, provision of advice and information to other bodies e.g. referrals to the panel for consideration of disqualification from working with children list under the Protection of Vulnerable Groups (Scotland) Act 2003. GTCS are also concerned with crime prevention and prosecution of offenders.

11.8.3

Chapter 12: Subject Access Requests

12.1 Introduction

12.1.1 Subject Access Requests are dealt with by the Response & Information Unit in Crown Office.

12.1.2 Where a person asks for a copy of their personal information which is held by COPFS, they should be asked to complete the Subject Access Request form(insert link http://www.copfs.gov.uk/images/Documents/Prosecution_Policy_Guidance/Guidelines_and_Policy/Subject%20Access%20Request%20form%202014.pdf) which is available on the website and submit it, together with two forms of identification to the Response and Information Unit to the _Subject Access Requests mailbox for attention.

12.1.3 All staff should have a general understanding of the Data Protection legislation and the Freedom of Information legislation and ensure that they are able to recognise a request when it is received in their office. RIU can provide advice and assistance and where it is established that a request falls under either the Data Protection Act or the Freedom of Information (Scotland) Act, will arrange for a response to be sent.

12.1.4 A central record of all Subject Access Requests is maintained by RIU. **Accordingly, RIU must always be advised when an office/division/department receives a Subject Access Request directly**, in order that the central record can be updated accordingly. This can be done by e-mailing the _Subject Access Requests common mailbox with details of the request.

12.2 Format of the Subject Access Request

12.2.1 In terms of the legislation, the request must be **in writing**. This can be by letter, fax e-mail or in the form of the Subject Access Form, which is available from the COPFS Website (copy attached at Annex B to this Manual).

12.2.2 Where a telephone enquiry is taken the applicant should be informed that a **written request is required** before the enquiry can be progressed.

12.2.3 The applicant should establish proof of their identity by providing copies of **two** official documents which between them clearly show the applicant's:

(a) Name;
(b) Date of Birth; and
(c) Current address

12.2.4 Notwithstanding the legislative requirement for the request to be in writing, in exceptional circumstances, it may be appropriate to waive this requirement, e.g. where the data subject has special needs that mean that a written request would not be appropriate.

12.3 Recording Receipt of the Subject Access Request

12.3.1 Where a Subject Access Request is received directly into a PF Office or Crown Office department, is should be passed immediately to the Response & Information Unit for logging, acknowledging, investigation and reply. Staff should use the _Subject Access Requests mailbox.

12.3.2 Subject Access Requests must be forwarded **immediately** to RIU as a response must be sent within the statutory period of **40 calendar days**.

12.3.3 RIU will log the request on Respond and acknowledge receipt within 3 working days.

12.3.4 RIU will prepare a response. Requests will be considered on an individual basis and where the request is complex or appears to be covered by an exemption will be subject to approval routes determined in Policy Division.

12.4 Is the Request a Subject Access Request or a Request under FOI?

12.4.1 The content of the request should be assessed to determine whether the request is for information in terms of the 1998 Act. The request may simply be a routine enquiry or may be a request for information in terms of the Freedom of Information (Scotland) Act 2002.

12.4.2 One request may invoke the terms of several pieces of legislation even where the applicant only makes reference to a particular regime, and must be treated accordingly.

12.4.3 Further guidance on determining whether a request is in terms of the Data Protection Act 1998 or the Freedom of Information (Scotland) Act 2002 is contained in Chapter 7 of this guidance.

12.5 What information is the Applicant seeking?

12.5.1 Where the terms of the request are not clear it may be necessary to clarify this with the applicant. Time spent clarifying the terms of a request will **not** be

calculated towards the 40-day response target; the 40-day time-limit starts running from the date that all the necessary information is received and the data controller is satisfied as to the identity of the applicant (and fee paid where necessary).

12.5.2 Under **Section 7(3)** of the 1998 Act, the data controller may only ask for further information in so far as it is reasonably required to locate the information sought by the data subject. Thus further questions may be asked but these should be directed towards and framed so as to refer to ways in which the data controller may more readily locate the information sought.

12.5.3 If a data subject refuses to supply further information reasonably required to enable the data controller to be satisfied of the identity of the data subject, then the data subject can no longer rely on Article 8 of the European Convention on Human Rights to defeat the **Section 7(3)** exemption.

12**.** 5.4 Note that the applicant is **not** required to state the purposes for the Subject Access Request or how s/he intends to use information obtained, as a result of the request.

12.6 Identifying the Information Requested

12.6.1 In order to locate all relevant information it will be necessary to consider all possible sources. As discussed, the information may be held manually and/or electronically. Examples include: correspondence; e-mails; reports; notes of meetings or telephone calls; photographs; and CCTV images.

12.6.2 The contents of each relevant item must be considered. Confidentiality markings are **not** to be treated as prescriptive. The terms of the 1998 Act apply to all personal data, even that which is identified as private or confidential or potentially embarrassing.

12.6.3 It will be necessary to identify whether data held manually forms part of a relevant filing system or is unstructured data.

12.6.4 Where the data is within a relevant filing system it will be easily located and the contents considered.

12.6.5 Where personal data is contained within an unstructured manual file, as defined by **Section 9A** of the 1998 Act, the data controller's obligations when responding to a Subject Access Request differ. These files are unstructured by definition making a search of the contents a potentially time-consuming exercise. The data controller is only obliged to comply with a Subject Access Request, **in so far as it relates to data within an unstructured file, where the applicant has provided a description of the information sought.** Even where the applicant has provided a description of the information the data controller can

refuse to comply with the request on the basis that the estimated cost of complying with the request would exceed £600.

12.7 Has the Information Been Destroyed?

12.7.1 The current Records Management policy relating to operational case records is contained within the Records Management Manual and in the records retention schedules. This guidance will be of assistance in determining whether case records held by COPFS should have been transmitted to the National Records of Scotland, or should have been destroyed.

12.7.2 The Manual and retention schedules will be a useful guide, but should not be treated as a substitute for making suitable investigations into specific storage arrangements.

12.7.3 Where data is held, however, that should have been destroyed in terms of the Records Management Policy but has not been so destroyed, the data must be considered for disclosure in the normal way.

12.8 Is disclosure of the data subject to any exemptions?

12.8.1 Where personal data has been identified as being held the next step is to assess whether that information should be supplied to the applicant. In short, it is necessary to consider whether any exemptions apply. For further details on exemptions see Chapters 5, 6 and 9 of this Manual.

12.9 Information relating to another Individual

12.9.1 Consideration should then be given to whether the information requested also contains information relating to another individual. Fuller guidance in relation to such disclosure is contained in Chapter 13 of this Manual

12.10 Format of Response

12.10.1 **The response should be in writing**, which may be by letter or email. In exceptional circumstances a large print or an audio response may be appropriate.

12.10.2 Where necessary, full guidance on interpreting, translating and transcription of material for persons with special needs can be found in the Diversity Guidance Manual. In cases of doubt, or where the Diversity Guidance Manual does not provide assistance, staff should contact the Diversity Team, Policy Division.

12.11 Content of Response

12.11.1 The response should contain the following information:

(1) The data subject should be informed whether any of their personal data is held;
(2) Where only part of their personal data is being disclosed, the data subject should be advised which exemptions were applied and in relation to which personal data;
(3) Details of the data subject's right to seek a review.

12.12 Format of Information Provided

12.12.1 If personal data is held it should be provided in an intelligible form; this should be in a permanent form unless this is not possible or would involve disproportionate effort or the data subject agrees otherwise.

12.12.2 There is **no** requirement to provide copy documents and the applicant has no right to demand sight of any documents held. **A summary of the information held is sufficient.** The data controller can choose whether to provide either a redacted copy of the actual document, showing only the personal data to which the individual is entitled or an intelligible communication which has been prepared for the purposes of the Subject Access Request containing the personal data.

12.12.3 Where an exemption applies the nature of the exemption should be explained. Standard paragraphs are available at Annex C.

.

12.13 Review

12.13.1 The response should include information about the applicant's right to seek a review by the Information Commissioner if they are unsatisfied with the response.

12.13.2 A standard paragraph is available at Annex C of this Manual.

12.14 Recording the Date of Disposal

12.14.1 The RIU team will log the date of disposal (i.e. the date the response is sent out) and place a copy of the reply on the Respond record.

12.15 Fee

12.15.1 The 1998 Act provides that up to £10 may be charged for providing information. It is COPFS departmental policy that no charge will be made for the first request for information under the Data Protection Act 1998, but that a fee may be charged for subsequent provision of information.

12.16 Repeated Requests

12.16.1 Where an applicant repeatedly submits a request for essentially the same information they should be referred to the previous correspondence and no further action is necessary.

12.16.2 However where a substantial period of time has passed it may be appropriate to reconsider the terms of the request.[17]

[17] **Section 8(3)** of the 1998 Act.

Chapter 13: Information relating to another Individual

13.1 General Principles

13.1.1 Often it is not possible to provide the applicant's personal data without disclosing information relating to a third party, who can be identified from that information. In these circumstances there is **no obligation to comply** with the request.[18]

13.1.2 **Steps should be taken to disclose as much information as possible through suitable editing or redaction.** When considering whether information relating to a third party should be disclosed, it is important to consider that even redacted information may render a third party identifiable when combined with information already known to the data subject, which would be in breach of the 1998 Act.

13.1.3 Where it is not possible to disclose an annotated version, the third party in question may consent to disclosure of their personal data. There is **no obligation to seek consent** and it may not always be appropriate, for example where this would disclose information about the data subject to the third party.

13.1.4 Alternatively, it may be reasonable to proceed without obtaining consent. In such circumstances, in terms of **Section 7(6)**, you should first consider:

(a) Whether any duty of confidentiality is owed to the other individual;
(b) Whether any steps have been taken by the data controller with a view to seeking the consent of the other individual;
(c) Whether the other individual is capable of giving consent, and
(d) Whether the other individual has expressly refused consent.

13.1.5 Where a decision is taken to disclose in the absence of consent you must keep a clear record of your reason for the decision.

13.2 Naming of Ministers, Officials and COPFS employees

13.2.1 The names of Ministers, officials or employees of COPFS may appear in documents together with opinions or advice that they have given (e.g. precognoser's notes). **Section 7** of the 1998 Act makes reference to "relating to another individual" (rather than the more narrowly framed "third party") which is of significance. "Third party" is defined in **Section 70** of the 1998 Act as meaning any party other than the data subject, the data controller or any data processor or other person authorised to process data for the data controller or processor. Under the wider definition of "another individual", Ministers, officials and COPFS

[18] **Section 7(4)** of the 1998 Act.

employees are not third parties of COPFS but are other individuals who themselves have certain rights to protect information that relates to them.

13.2.2 Although section 7 of the 1998 Act places the emphasis on compliance with a subject access request so far as possible (and sometimes even without the consent of the other individual), care should be taken to ensure that reasonable steps are taken to protect the rights of Ministers, officials and COPFS employees. Section 7(5) expressly allows redaction, although this must be considered on the facts and circumstances of each individual request. The rights of the other individual may alternatively be protected through provision of annoymised data. It is also appropriate to consider obtaining consent from the other individual to the provision of the requested information to the data subject.

13.2.3 Where the other individual is an employee of COPFS or a Senior Official within the Department, consent should always be sought prior to refusing to provide information to the data subject as it would be very straightforward to make such a request.

13.3 Disclosure without the consent of the other individual

13.3.1 Where the provision of information to the data subject would also disclose information relating to another individual, you must conduct a balancing exercise in order to determine whether the information relating to the other individual should be disclosed. The factors to be taken into account could properly include the nature of the reason for the subject access request, the nature of the information in question, expectations as to the level of disclosure public servants ought to be prepared to endure and possible detriment to efficient government in politically sensitive areas.

13.3.2 It should be noted that the test for disclosure without the consent of the other individual is an objective test and, accordingly, a court would be entitled to form its own view on what was reasonable in the circumstances.

13.3.3 Section 7(6) of the 1998 Act provides that, when determining whether to disclose information without consent, regard must be had to any duty of confidentiality owed to the other individual. This obligation of confidence arises where the information in question is not known to others and was imparted in circumstances which lead to an expectation of confidentiality. Accordingly, a duty of confidence may arise in relation to internal memoranda, letters and other documentation written by or referring to Government Ministers and other senior officials. This will be a matter of facts and circumstances in relation to each piece of information and is unlikely to apply as a matter of routine.

13.4 Recipients of Information

13.4.1 **Section 7(1)(b)(iii)** provides that an individual is entitled to be given a description of the recipients or classes of recipients to whom personal data has or may be disclosed.

13..4.2 Where Ministers, Senior Officials or COPFS employees are mentioned in documents merely as recipients or copy recipients and that person's name does not *otherwise* constitute personal data to which the data subject is entitled, then the data controller should given the data subject a description of the recipients or classes of recipients.

13.4.3 **Section 70** of the 1998 Act defines "recipient" as *"any person to whom the data is disclosed including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law".*

13.4.4 Arguably, the reference to "recipients or classes of recipients" gives the data controller a choice between providing individual names of recipients or a generic description of the recipients.

13.4.5 It is important to note that in terms of the European Directive and the 1998 Act, the right to a description of recipients and the right under **Section 7(1)(c)(i)** of the 1998 Act to information are separate rights which impose different obligations on the data controller.

Chapter 14: Offences under the Data Protection Act 1988

14.1 Introduction

14.1.1 The 1998 Act creates a number of criminal offences. The main offences are:

- Offences under **Section 21** of the 1998 Act, namely:
  - Contraventions of **Section 17(1)**
  - Contraventions of **Section 20(1)** – failure to comply with the duty imposed by notification regulations
- **Section 47** of the 1998 Act - failure to comply with a notice
- **Section 55** – unlawfully obtaining etc of personal data

14.2 The Information Commissioner may submit reports to the relevant PF Office for the consideration of criminal proceedings.

14.3 Contraventions of Section 17(1)

14.3.1 **Section 21** of the 1998 Act provides that, where a data controller, contravenes **Section 17(1)**, s/he is guilty of an offence.

14.3.2 **Section 17(1)** provides that personal data must not be processed unless an entry in respect of the data controller is included in the register maintained by the Commissioner under **Section 19**.

14.3.3 A data controller found guilty of such a contravention is liable on summary conviction to a fine not exceeding the statutory maximum and on indictment to a fine.

14.3.4 A specific case marking guidance note on **section 17(1)** of the 1998 Act can be accessed in the Case Marking Guidance Manual.

14.4 Contraventions of Section 20 (1)

14.4.1 **Section 21** of the 1998 Act provides that any person who fails to comply with the duty imposed by notification regulations made by virtue of **Section 20(1)** is guilty of an offence.

14.4.2 **Section 21(3**) provides that it is a defence for a person charged with an offence under subsection (2) to show that s/he exercised all due diligence to comply with the duty.

14.4.3 A person found guilty of a contravention of **Section 20(1)** is liable on

summary conviction to a fine not exceeding the statutory maximum and on indictment to a fine.

14.4 Failure to Comply with a Notice (Section 47)

14.4.1 Under **Section 47(1)**, a person who fails to comply with an enforcement notice, an information notice or a special information notice is guilty of an offence. **Section 47(2)** provides that a person who, in purported compliance with an information notice or a special information notice (a) makes a statement which s/he knows to be false in a material respect, or (b) recklessly make a statement which is false in a material respect is guilty of an offence.

14.4.2 It is a defence for a person charged with an offence under subsection (1) to demonstrate that all due diligence was exercised to comply with the notice.

14.4.3 A person found guilty of a contravention of **Section 47(1)** or **(2)** is liable on summary conviction to a fine not exceeding the statutory maximum and on indictment to a fine.

14.5 Unlawfully Obtaining etc of Personal Data (Section 55(1))

14.5.1 **Section 55(1)** & **(3)** provide that it is an offence to knowingly or recklessly, without the consent of the data controller:

(a) Obtain or disclose personal data or the information contained in personal data; or
(b) Procure the disclosure to another person of the information contained in the personal data.

14.5.2 Under **subsection (2)**, **section 55(1)** does not apply to a person who shows:

(a) That the obtaining, disclosing or procuring –
    i) Was necessary for the purpose of preventing or detecting crime, or
    ii) Was required or authorised by or under any enactment, by any rule of law or by the order of a court
(b) That s/he acted in the reasonable belief that s/he had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person;
(c) That s/he acted in the reasonable belief that s/he would have the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring the circumstances of it, or
(d) That in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

14.5.3 **Section 55(4)** of the 1998 Act provides that a person who sells personal

data is guilty of an offence if s/he has obtained the data in contravention of subsection (1).

14.5.4 In terms of **Section 63(5)** of the 1998 Act, a government department shall not be liable to prosecution under the Act. However, **persons in employ of the Crown may be prosecuted in terms of Section 55 and for intentional obstruction of the execution of a warrant in terms of Schedule 9, Paragraph 12.** For an example of a servant of a data controller being prosecuted see ***McGregor v McGlennan***[19], in which a Strathclyde Police Officer was charged as an agent or servant of the Chief Constable with a contravention of **Section 5(3)** of the Data Protection Act 1984[20].

14.5.5 A person found guilty of a contravention of **Section 47(1)** or **(2)** is liable on summary conviction to a fine not exceeding the statutory maximum and on indictment to a fine

14.5.6 A specific case marking guidance note on **Section 55** of the 1998 Act can be accessed in the Case Marking Guidance Manual.

[19] 1993 SCCR 852
[20] This being the equivalent section under the 1984 Act

Annex A

DEFINITIONS AND KEY CONCEPTS

1. Section 1 of the 1998 Act

Data means information which-

(a) is processed by means of equipment operating automatically in response to instructions given for that purpose
(b) is recorded with the intention that it should be processed by means of such equipment
(c) is recorded as part of relevant filing system or with the intention that it should form part of a relevant filing system, or
(d) does not fall within paragraphs (a), (b) or (c) but forms part of an accessible record[21].
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)…" [Subsection added by the Freedom of Information Act 2000, Section 68 – commencement 1 January 2005]

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data subject means an individual who is the subject of personal data.

Personal data means data which relate to a living individual who can be identified –

(a) from those data, or
(b) from information which is in possession of, or likely to come into the possession of, the data controller

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Processing in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

[21] Health and educational records in terms of **Section 68** of the 1998 Act or accessible record as defined by **Schedule 12** (Paragraph 4, insofar as this relates to Scotland).

(d) alignment, combination, blocking, erasure or destruction of the information or data.

Relevant filing system means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

2. Section 2 of the 1998 Act

Under Section 2 of the Act ***sensitive personal data*** means personal data consisting of information about –

(a) racial or ethnic origin;
(b) political opinions;
(c) religious or similar beliefs;
(d) trade union membership;
(e) physical or mental health or condition;
(f) sexual life;
(g) commission or alleged commission by him of any offence or;
(h) proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence in such proceedings.

3. Section 3 of the 1998 Act

Special Purposes means any one or more of the following:

(a) the purposes of journalism;
(b) artistic purposes; and
(c) literary purposes

4. Section 9A of the 1998 Act

Unstructured personal data means any personal data falling within paragraph section (1)(1)(e) above, other than information which is recorded as part of, or with the intention that it should form part of, any set of information relating to individuals to the extent that the set is structured by reference to individuals or by reference to criteria relating to individuals.

5. Section 68 of the 1998 Act

Accessible Record means:

(a) a health record as defined by section 68(2);
(b) an educational record as defined by Schedule 11 of the 1998 Act; or
(c) an accessible public record as defined by Schedule 12 of the 1998 Act

Health Record means any record which:

(a) consists of information relating to the physical or mental health or condition of an individual; and
(b) has been made by or on behalf of a health professional in connection with the care of that individual.

6. Section 71 of the 1998 Act

The 1998 Act defines a large number of different expressions throughout the Act. A full index of those defined expressions is contained in section 71.

Annex B

DATA SUBJECT ACCESS REQUEST APPLICATION

SECTION 1 – ABOUT YOURSELF

The information we ask for below is to help the Crown Office and Procurator Fiscal Service to (a) satisfy ourselves as to your identity and (b) find any data about you that we have.

FULL NAME	
MAIDEN NAME (if applicable)	
	MALE ☐ **FEMALE** ☐
DATE OF BIRTH	
PLACE OF BIRTH	**TOWN:** **COUNTY:** **COUNTRY:**
CURRENT ADDRESS	

SECTION 2 – INFORMATION REQUIRED

Please provide as much of the following information as you can.

Were you	**An accused in any criminal case?** ☐ **A victim or witness in any criminal case?** ☐ **Other?** ☐
If other, please specify details	
Name of Accused (if not you)	
Offence(s) accused was prosecuted for	
Case Reference Number	
Procurator Fiscal Office that dealt with the case	
Name of Court	
Approximate date when case was last in court	
Any other information that you can provide about the case	

Please specify the particular information you are looking for. If you ask for "all information held about me" your request is likely to be refused as being for unstructured data in terms of the Data Protection Act 1998.

SECTION 3 – PROOF OF IDENTITY

To help establish your identity copies of TWO official documents must be sent with your application form. These documents between them must show:

- **Your name;**
- **Date of birth; and**
- **Current address**

for example a photocopy of a driving licence, birth/adoption certificate, passport or any other official document, which shows your name and address.

Declaration – To be signed by the applicant

The information which I have supplied in this application is correct and I am the person to whom it relates.

Signature: Date:

Warning

A person who impersonates or attempts to impersonate another with the intention of obtaining information to which he or she is not entitled may be guilty of an offence.

Please send completed forms to:

The Response & Information Unit
Policy Division
Crown Office
25 Chambers Street
Edinburgh
EH1 1LA

General advice on the Data Protection Act 1998 can be obtained from:

The Information Commissioner
Wycliffe House

Walter Lane
Wilmslow
Cheshire
SK9 5AF

Annex C

STYLE PARAGRAPHS

Exemption under section 29 of the Data Protection Act 1998

[Some of the] [The] information requested relates to ongoing criminal proceedings, and is exempt from disclosure in terms Section 29 of the Data Protection Act 1998. This section exempts personal data processed for either (a) the prevention and detection of crime, or (b) the apprehension or prosecution of offenders where the provision of data in terms of Section 7 of the Act would be likely to prejudice any of these matters.

We have considered [this part of] your request and determined that providing this information [could lead to the identification of witnesses and] could be prejudicial to the ongoing prosecution. Accordingly, we are unable to comply with [this part of] your request.

Right of the applicant to contact the Information Commissioner

If you consider that your request [for access to your personal data] has not been dealt with in accordance with the Data Protection Act 1998 you may write to the Information Commissioner who may do any of the following:

1. make an assessment as to whether it is likely or unlikely that the Department has complied with the Data Protection Act 1998;
2. take enforcement proceedings if the Commissioner is satisfied that the Department has contravened one of the Data Protection principles;
3. recommend that you apply to court alleging failure to comply with the subject access provisions of the 1998 Act.

The Information Commissioner's Office (ICO) is based at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF and the ICO website can accessed at www.ico.gov.uk. (Contact telephone numbers: Switchboard - 01625 54 57 00 / ICO Helpline – 08456 30 60 60 or 01625 54 57 45.)

Annex D

Comparative Rights Of Access Under The Data Protection Act 1998 & Freedom Of Information (Sc) Act 2002 *(reproduced from the Freedom of Information (Scotland) Act 2002 Guidance Manual, volume 1)***.**

Note – In relation to the Data Protection Act these notes do not deal with the special rules which apply for access to accessible records.

ISSUE		**DATA PROTECTION**	**FREEDOM OF INFORMATION**
1.	Who can apply for information?	Only the data subject that is the living individual to whom the particular data relate.	Anyone anywhere can apply for information. This can include limited companies or persons who are overseas.
2.	Who can a request be made to?	Any data controller that is a person or organisation within the public or private sector who determines the manner and purpose of the processing as long as the controller is subject to UK law.	Any Scottish public authority listed in the FOISA.
3.	Can the organisation ask for proof of the identity of the applicant?	Yes, it must do so as the data controller is under an obligation not to disclose information to an unauthorised third party.	No, the applicant must give a name and an address for correspondence but in most cases the identity of the applicant is irrelevant. However, if special circumstances apply for example the applicant is suspected of making vexatious or repeat applications then the identity of the applicant may be relevant. Also, the identity of the applicant may be relevant when making a request for a review to a

ISSUE		DATA PROTECTION	FREEDOM OF INFORMATION
			public authority.
4.	How must an application be made?	In writing, this means in a form which gives rise to a permanent record although this may be by e-mail or other electronic mechanism.	In writing, this means in a form which gives rise to a permanent record although this may be by e-mail or other electronic mechanism.
5.	What information can be requested?	All the information which relates to the data subject and which falls with the definition of data in the DPA, that is broadly information held on a computer or in a filing system in which specific information about the individual can be readily found**.** It also covers structured files in which specific information cannot be readily accessed and unstructured information.	Any recorded information held by or on behalf of the authority.
6.	Can a fee be charged?	Yes. Generally a fee of up to £10 can be charged.	Yes, authorities will be able to charge a fee in accordance with Fees Regulations.
7.	When is the fee payable?	When the request is made or prior to the information being provided.	If an authority wishes to charge a fee once it has received a request, it must give the applicant a fees notice. The specified fee must be paid before the authority actions the request for information.
8.	How specific does the request have to be?	The request must enable the authority to locate the information requested. If	The request must enable the authority to locate the information requested. If this is

ISSUE		DATA PROTECTION	FREEDOM OF INFORMATION
		this is not possible the authority can ask the subject to provide further information and does not have to respond until it has received enough information to handle the request.	not possible the authority can ask the subject to provide further information and does not have to respond until it has received enough information to handle the request.
9.	Is there a limit to the amount of information that can be requested?	No, the individual is entitled to all the personal data held about him/her unless it is exempt.	Yes, there is a limit to the searching which an authority must carry out to provide the information. This is set as the appropriate limit.
10.	Does the organisation always have to answer a request for information?	It should always send a reply but in some circumstances it does not have to acknowledge that it holds information.	It should always send a reply but in some circumstances it does not have to acknowledge that it holds information.
11.	Must original documents be provided?	No, the individual is entitled to the information constituting the data not a copy of the actual data.	No, the obligation is to provide information not to provide copy documents.
12.	Can the applicant insist on having the information in a particular form or format?	No, however, codes must be explained. If it is not possible to provide the information in permanent form without disproportionate effort the information can be provided by other means e.g. inspection.	No, the applicant cannot insist but can specify a preferred form when making the request. An authority must accommodate the request if practicable and if it is not practicable explain why.
13.	How long does the organisation have to	The organisation must respond as soon as possible and in any event within **40 calendar days** of receiving a valid	The authority must respond within **20 working days**.

ISSUE		DATA PROTECTION	FREEDOM OF INFORMATION
	respond to a request?	request and fee.	
14.	Are there any exemptions from the obligation to provide information?	Yes, there are a range of exemptions set out in the Act. These are usually applied on a case by case basis.	Yes, there are exemptions set out in the Act.
15.	Can information be excluded or blacked out ("redacted") from documents supplied in response to a request?	Yes, if the information relates to another individual and it is not reasonable to give it or an exemption applies. Where information can be redacted that should be done rather than withholding information.	Yes, information can be redacted if it is exempt. Information should be redacted rather than access being refused.
16.	What recourse or remedy is there if the authority does not provide the information it should?	The individual can either complain to the Information Commissioner's Office (UK Commissioner) or can go to court.	The complainant must make a request for review to the authority which will reconsider the application. If not satisfied it can be referred to the Scottish Information Commissioner. The Scottish Information Commissioner's decision can then be appealed to the Court of Session.

Annex E

SUBJECT ACCESS REQUESTS FLOWCHART