DWP Department for Work and Pensions

Personal Information Policy

(An overview of the policy principles to be considered when DWP staff disclose personal customer information to a third party)

Produced by:
Adjudication and Constitutional Issues Information Division
(Data Protection and Freedom of Information Section).

This version dated 01 December 2003

Foreword

As we all know, the Department for Work and Pensions is one of the largest holders of personal information in the UK. The correct handling of this information is of major importance. Our customers need to be confident that DWP treats their personal information as confidential and with respect.

Information handling within the Department is governed by the Data Protection Act; the Code of Practice on Access to Government Information ("Open Government"); Freedom of Information legislation; internal security requirements; and, not least, our general policy on confidentiality. In addition, the Civil Service Code places duties on staff concerning the handling of information. This document brings all of these obligations together, setting out the DWP policy on handling personal information. **It must be followed by all staff within the Department**.

The correct handling of information will help to ensure that the Department aims for, and meets, Government requirements to improve the quality, accuracy and security of the services we provide to all our customers. In turn this will instil confidence in our customers that we are managing their personal information with due care.

We need to strike a balance between the duties placed upon us all to protect customer information **and** to disclose that information where it is appropriate to do so. This policy document sets out the principles underpinning any decision to disclose personal information and will enable you to strike that balance.

Following these principles will help protect you from making unlawful disclosures, as well as ensuring that the department adequately protects the vast amounts of personal information it holds.

This document replaces the Protection of Customer Information Guide (PCIG) which should no longer be used or referred to. The principles set out in this document will be underpinned by Agency specific operational guidance implementing these principles.

Further information about this document can be obtained from the DWP Policy team responsible for disclosure, confidentiality, Data Protection and Freedom of Information (Adjudication and Constitutional Issues Information Division (Data Protection and Freedom of Information Section)) either from their Intranet site (ACI (inf) DP & FoI Intranet site) or by telephone to Charles Cushing (020 7962 8581) or Martin Dillon (020 7962 8633).

Marilynne A Morgan
Law and Special Policy Group
1 December 2003

ABBREVIATIONS

ACI (Inf)	Adjudication & Constitutional Issues (Information)
ACIS	Adjudication & Constitutional Issues (Scotland)
ACPO	Association of Chief Police Officers
ACPOS	Association of Chief Police Officers in Scotland
tAS	the Appeals Service
BFLS	Bulk Letter Forwarding Service
CAB(x)	Citizens Advice Bureau(x)
CDA	Crime and Disorder Act 1998
CFID	Counter-Fraud Investigation Division
CFIS	Counter-Fraud Investigation Service
CRU	Compensation Recovery Unit
CSA	Child Support Agency
CTB	Council Tax Benefit
DDPU	Departmental Data Protection Unit
DLA	Disability Living Allowance
DP	Data Protection
DPA	Data Protection Act 1998
DWP	Department for Work and Pensions
EO	Executive Officer
FoI	Freedom of Information
GBU	General Benefit Unit
GP	General Practitioner
HB	Housing Benefit
HEO	Higher Executive Officer
HRMC	Higher Rate Mobility Component (of DLA)
HRU	Human Resources Unit
LA	Local Authority
LSC	Legal Services Commission
MAGU	Monitoring and Guidance Unit (CSA)
MIDAS	Matching Intelligence and Data Analysis Service
MoU	Memorandum of Understanding
MP	Member of Parliament
MSP	Member of Scottish Parliament
NHS	National Health Service
NINo	National Insurance number
OIU	Operational Intelligence Unit
PCIG	Protection of Customer Information Guide
PF	Procurator Fiscal
PV	Potentially Violent
(T)PS	(The) Pension Service
RAT	Remote Access Terminal
SAR	Subject Access Request
SSAA	Social Security Administration Act 1992
SSFA	Social Security (Fraud) Act 1997
UCB	Unacceptable Customer Behaviour

CONTENTS

Part 1 – Fundamental Principles

Part 2 – Guidelines to applying the Principles in Part 1

Appendix 1 – Local Authorities

Appendix 2 – The Police

Appendix 3 – Representatives

Appendix 4 – Miscellaneous

Appendix 5 - Criminal offences relating to the misuse of personal data

[This page left blank]

PART 1

FUNDAMENTAL PRINCIPLES

1. Introduction

1.1 This document outlines the principles to be applied by Department for Work and Pensions (DWP) staff when considering whether to disclose personal information about customers to someone who is not the customer. **All staff in the Department must use it** when dealing with requests for personal information relating to our customers or staff. **It is the primary source of the policy principles within the department** on when personal customer information may be passed to third parties and **replaces the Protection of Customer Information Guide (PCIG)**, issued in April 2000, **which must no longer be used.**

1.2 If you unlawfully disclose information you could be held personally liable. This document aims to help you make informed decisions and respond to requests for information without breaking the law or Departmental policies. **Following the principles in this document will protect you from unlawful disclosure, as well as ensuring that the Department adequately protects the vast amounts of personal information it holds**. Appendix 5 sets out some of the criminal offences relating to the misuse of personal information. Additional guidance about the release of personal information can be found on the Adjudication and Constitutional Issues Data Protection and Freedom of Information (ACI INF (DP/FoI) Intranet site (ACI (DP & FoI) Intranet site). Contact details can be found at Part 2 paragraph 7.5.

1.3 Guidance on the release of non-personal information i.e. under the Code of Practice on Access to Government Information (Open Government) or the Freedom of Information Act can be found on the ACI INF (DP/FoI) Intranet site:
Open Government
ACI (DP & FoI) Intranet site

1.4 Disclosure is a decision-making process involving complex issues and considerations. It is recognised that such decisions are not always easy and this document concentrates on the underpinning principles which must be considered when weighing up our duty of confidentiality to customers, clients and staff against the need to disclose personal information.

1.5 The diversity of our business makes it extremely difficult to produce comprehensive operational guidance covering every possible scenario that may occur. Each request must be considered on its own merits. Therefore this document does not attempt to offer prescriptive direction on handling specific individual requests; rather it lays out what considerations must be taken into account in reaching a decision. Following the basic principles in every case; documenting the facts; the decision reached and the reasoning behind it will ensure that disclosures are only made where appropriate or permissible. In turn this will instil confidence in our customers that we are managing their personal information with due care.

1.6 ACI INF (DP/FoI) are aware that disclosure decisions are not always straightforward and that the penalties for inappropriate disclosure can be serious. Therefore help and advice is available to all staff from the advice line run by ACI INF (Departmental Data Protection Unit) [DDPU]. Contact details can be found at Part 2 paragraph 7.6

1.7 Also detailed at Part 2 paragraph 7.6 are the main Departmental contacts for disclosure and confidentiality issues. Specialist business units will produce their own guidance on

how to put this document into operational use. Individual business unit guidance will include relevant contact points for that particular area of work.

2. Layout of this Document

2.1 The main body of this document sets out the fundamental policies underpinning all disclosures of personal information to third parties. It is followed by a number of appendices relating to areas of particular concern or difficulty. This approach has been taken as the underpinning policies do not change whilst accepting that actual implementation of the policies may well be dependent upon a number of operational considerations. **It is not possible to anticipate all circumstances in which the Department may be approached for information**. If you receive a request which is not covered in this policy document please contact DDPU or your nominated business unit representative.

3. Who should use this Document?

3.1 The principles contained within this document are to be followed **by all staff** who may need to make decisions on the disclosure of personal information. **This applies irrespective of which part of the Department you work in**.

3.2 However, whilst the principles contained within this document underpin **all** disclosures of personal information there are circumstances where reference may also need to be made to more detailed and specific business unit guidance. Such guidance will always be compliant with the overarching principles laid out in this document. Examples where other guidance may be issued, reflecting unique operational or legislative requirements, include the Child Support Agency (CSA), the Pensions Service (TPS), the Appeals Service (TAS) and Jobcentre plus (e.g. fraud). Additionally, ongoing and updating guidance will be issued through benefit bulletins, Counter Fraud Management Letters and articles in Newsreel etc.

3.3 Whilst this policy document sets out the basic principles to follow in respect of disclosing personal information **it is primarily to be used in respect of individual requests rather than bulk requests or requests for data matching or scans**. Enquiries in relation to bulk requests, data matching or scans should be referred to Matching Intelligence and Data Analysis Service (MIDAS). Information on the role of MIDAS can be found by clicking role of MIDAS. Contact details for MIDAS can be found at Part 2 paragraph 7.5. If a bulk request does not fall within the remit of MIDAS please contact ACI INF (DP/FoI) who will consider whether the request raises any policy issues and will direct the enquiry to the appropriate business unit.

3.4 Detailed guidance on the statutory gateways allowing disclosures between DWP and other government departments and bodies including Local Authorities can be found on the ACI INF (DP/FoI) Intranet site. To access this information, click here: Statutory Powers for Data Sharing

3.5 There is increasing interaction between DWP and the Inland Revenue and specific legal gateways are in place to facilitate the exchange of information. These gateways can be found on the Intranet site mentioned at paragraph 3.4.

3.6 Information held by one government department or agency for a particular function can usually only be used for the purpose for which it was collected or given and cannot be shared as a matter of course with other public (or private sector) bodies. Always check with ACI INF (DP/FoI) if you are unsure.

3.7 Under the Modernising Government agenda, the introduction of legislation to permit the exchange of information continues to establish new legal gateways. To view current legislation, click here: Statutory Powers for Data Sharing

3.8 The Modernising Government agenda does not, of itself, provide a legal gateway until or unless legislation is introduced to permit the exchange of information.

4. Closer working and permissive legislation

4.1 Local Authorities (LAs) or other service providers may want access to DWP information or require DWP to obtain information from another body on their behalf, to enable them to identify potential beneficiaries. Advice should always be sought from ACI INF (DP/FoI) when considering what role DWP can play in these initiatives, if any.

5. What is the Document?

5.1 It describes DWP Policy on the disclosure of personal customer information. It explains the balance necessary between obligations on the Department and its employees to protect personal customer information, and the need to disclose that information to someone other than the individual customer when it is lawful and necessary to do so.

5.2 You may receive many different kinds of requests for personal information and from a variety of sources. Decisions to disclose will depend on the provisions in a number of regulations, enactments, common law and Departmental policies. These include:

- Social Security Administration Act 1992 (sections 122 & 123)
- Child Support Act 1991
- DWP policy on the protection and disclosure of information, incorporating duties placed on us by, amongst other things, the Civil Service Code and internal security requirements
- Common law duties of confidentiality
- Data Protection Act 1998
- Computer Misuse Act 1990
- Human Rights Act 1998
- Code of Practice on Access to Government Information (Open Government)
- Freedom of Information Act 2000

5.3 This document takes account of Departmental policy and legislative considerations. **Following the principles and guidance in this document, and seeking further advice where it recommends you do so or where there is ANY doubt about a disclosure, means that the disclosures (and refusals to disclose) will comply with DWP policies and other relevant requirements.**

6. Departmental Policy

6.1 The Department's guiding principles are of fairness, even-handedness and compliance with the law. Staff must ensure that they:

- act lawfully
- comply with both the letter and spirit of relevant enactments
- meet common law duties of confidentiality **and**
- honour the Department's policy and principles on disclosure

Adherence to the guidance within this document will ensure such compliance.

6.2 The Department is a major custodian of personal information and it is important that customers, individually and collectively, are confident that we hold their personal information securely, and use it only for the purposes for which we are permitted to use it. In order to maintain this customer confidence, DWP holds that:

All personal information held by the Department is regarded as confidential. Information will not normally or routinely be disclosed to third parties without the consent of the person concerned.

6.3 However, information **may** be disclosed without consent in certain circumstances including:

- where required by statute - details of the statutory powers for exchanging information can be found here: Statutory Powers for Data Sharing **or**
- where permitted by statute (but **only** if the disclosure is fully in line with Departmental policy and this document – please refer to the ACI INF (DP/FoI) Intranet site as per the previous bullet point) **or**
- to comply with a court order **or**
- to prevent the duplication of payments from public funds (where there are specific statutory gateways for the disclosure of the information) **or**
- when there is a compelling public interest in making the disclosure (see paragraph 7) - adherence to this guidance will assist in assessing the public interest test.

6.4 This policy forms the basis of the guidance contained throughout this document. **All** disclosures made by DWP, in order to be considered authorised, must be able to demonstrate that at least one of the above criteria apply. Any disclosure must have a sound legal footing and comply with the Data Protection Act (DPA) Principles.

7. Public interest

7.1 The public interest test mentioned at paragraph 6.3 requires an assessment of whether, in any particular case, there are sufficiently strong grounds to justify overruling our duty of confidentiality to our customers.

7.2 It is widely accepted that it is impossible to define the public interest in such a way to meet all possible circumstances. However the public interest test is a strong one and is not easily satisfied. Where this guidance permits disclosure, you can safely assume that the public interest test has been met, but only after taking into account all circumstances relevant to the actual individual enquiry.

7.3 In case of any doubt at all, whether on the application of the public interest test or any other uncertainty about its application, please seek further advice.

8. Legal Background

Common Law

8.1 The law consists of common law, statute law and regulations authorised by statute. Common law is the body of law which is derived from judicial decisions rather than statutes or subordinate legislation.

8.2 Personal information is usually given to the Department for a specific purpose, and as such attracts a common law obligation of confidentiality. As a general rule, in the absence of consent personal information given for one purpose cannot be used for another purpose or disclosed to a third party. Where disclosure is in the public interest it may be possible to disclose information which is confidential at common law without that person's consent, but this is a limited exception to the general rule.

8.3 In Scotland, Common Law has a different meaning and application. It is more a "breach of confidence" where a relationship of confidentiality exists; e.g. like the relationship between doctor and patient. If you require further information on this subject, please contact ACIS.

8.4 It should also be remembered that the use of personal information is also governed by Social Security legislation and the DPA. These are collective and should always be considered before making a decision.

Departmental Legislation

8.5 DWP has included in its own legislation specific references to the disclosure of information. These references make unauthorised disclosure of departmental information a criminal offence and are at section 123 of the Social Security Act 1992 and section 50 of the Child Support Act 1991 (see Appendix 5 paragraphs 1- 5).

8.6 For disclosure to be considered authorised, it must be made either with the informed consent of the customer, or because one of the reasons outlined at para 6.3 applies.

Data Protection Act 1998 (DPA)

8.7 The DPA allows for information to be disclosed where:

the disclosure is exempt from the 'non-disclosure' provisions of the Act.

8.8 Broadly, the non-disclosure provisions impose some restriction on disclosure of personal data. The Act contains a number of exemptions, which allow data controllers (DWP in this case) to disclose personal data in limited circumstances notwithstanding these non-disclosure provisions. **The exemptions are only available on a case by case basis**, once we have evaluated all the circumstances and reached the view that the particular non-disclosure provision is incompatible with the disclosure in question and this disclosure falls within the terms of the relevant exemption.

8.9 All disclosures must have a sound legal footing AND comply with the DPA Principles. A brief introduction to the DPA can be found here: Data Protection Act 1998

8.10 The exemptions within the DPA allow for information to be disclosed:

- between DWP business units, where it is **essential** to allow DWP employees to conduct their legitimate business (such disclosures are also permitted by section 3 of the Social Security Act 1998, which provides that information relating to social security and child support can be shared for the purposes of DWP, see relevant entry at: Statutory Powers for Data Sharing

- where it is necessary for the prevention or detection of a crime or the apprehension or prosecution of offenders – for this exemption to apply it must be shown that there is a substantial chance rather than a mere risk that in any particular case failure to disclose the information would be likely to prejudice the purpose for which it is being requested (see Appendix 2 for further information about disclosing to police forces)

- for the assessment or collection of any tax or duty (including Council Tax) and where failure to disclose would be likely to prejudice this purpose

- where the disclosure is required by statute, rules of law or by an order of the court

- where the disclosure is necessary for the purpose of obtaining legal advice, or establishing, exercising or defending legal rights **or**

- where the disclosure is required to prevent injury or damage to anyone's health (this relates to protecting the vital interests of a person and the risk or harm must be more than minor e.g. a serious threat).

Where these exemptions are used or quoted, evidence MUST be provided to show that the criteria are met. Where no evidence is provided, or the evidence is insufficient, customer information must not be disclosed. Again, in the case of ANY doubt please seek further advice BEFORE disclosing information.

Other permissive legislation

8.11 Departmental legislation enables the Department to obtain information from other government departments as well as other bodies. Other government departments have sought their own legislative provisions allowing them to gain access to DWP information.

8.12 Details of legislative provisions relating to the disclosure of personal information both to and from DWP, can be found on the ACI (inf) DP & FoI Intranet site, or by clicking:

disclosure of personal information and Statutory Powers for Data Sharing.

In view of the number of new initiatives being developed it is important that this site is consulted and that further guidance is sought from ACI INF (DP/FoI) as appropriate.

Crime and Disorder Act 1998 (CDA)

8.13 The Crime and Disorder Act 1998 (CDA) established partnerships between:

- the police
- local authorities
- probation service
- health authorities
- the voluntary sector
- local residents
  and
- businesses
  (note: **not DWP**)

8.14 The CDA obliges these authorities to develop and implement strategies to reduce crime and disorder in each district and unitary local authority in England & Wales.

8.15 The CDA is not just about personal information - DWP ought to help (and do) where we can, for example in providing aggregated/anonymised information to inform audits of local crime and disorder problems. In all disclosure/confidentiality issues, DWP works within relevant legal parameters, our own policy on confidentiality and common law requirements. DWP will always assist police forces where we are enabled to do so (see Appendix 2 regarding disclosures to the police); the CDA does not change this.

8.16 Section 115 of the Act authorises any person to provide information to the police or local/health/probation authorities subject to the Act, which is necessary or expedient for the purposes of the Act. The Information Commissioner has confirmed that section 115 **does not impose a duty to disclose** and that any disclosure under these provisions must have regard to common law and statutory restrictions on disclosure including, but not restricted to, the DPA.

8.17 It is not appropriate for DWP staff to enter into any protocols under the CDA or to sit on any panels set up under the Act.

8.18 If you receive any request for information quoting section 115 please contact the DDPU. **Do not agree to provide assistance without first seeking advice from the DDPU**.

9. Personal and Departmental responsibility

9.1 If you act properly and within your authorised duties, fully following this and other relevant instructions, liability for any breach of confidence would normally lie with the Department. If DWP policies and guidance have been followed, the Department will fully support you in any claim or complaint that may be brought. If the decision to disclose is not within your personal authority, or disclosure was made contrary to this guidance, then both the Department and the individual may be deemed liable.

9.2 If, after consulting this document, you are still uncertain about whether information should be disclosed, seek further advice from the DDPU.

10. Information about staff

10.1 **Any request for information about a member of staff** must be referred to the relevant Human Resources Unit (HRU) for further advice. Do **not** provide any information or supply any documents without consulting the relevant HRU.

11. Media

11.1 Any requests for information from the media must be referred to your regional press and publicity officer. Contact details can be found on the Intralink under “Corporate and Shared Services, Communications Directorate, useful contacts” or by clicking: Communications site - useful contacts

National Press Office
2nd Floor
Richmond House
Whitehall
London
SW1A 2NF
020 7238 0866

12. Statistical Information

12.1 For advice on the disclosure of statistical information including management information, or requests from research organisations, you should contact the Central Data Unit (part of Financial Services Division; address below) or view the site on the Intralink under Corporate and Shared Services, Codes and Manuals, Management and Resources Statistics Guide (Management and Resource Statistics Guide).

The Central Data Unit
Room 205
Norcross
Telephone: 01253 330430

PART 2

GUIDELINES TO APPLYING THE POLICY PRINCIPLES IN PART 1

1.1 There are a number of basic issues to consider whenever a request for personal information is received; these are set out below.

1.2 **What needs to be considered before releasing personal information?**

- who is asking for the information – are they who they say they are? (see paragraphs 1.4 to 1.6)
- can you establish that consent has been provided? (see paragraphs 1.7 to 1.9)
- if consent is not provided can you still disclose? (see paragraph 1.10)
- relevance of the information requested or disclosed (see paragraph 1.11 to 1.12)

1.3 **Every request for personal information about our customers must be considered on an individual basis, taking all factors in the case into account.** The following must **always** be considered when any request for information is received.

Who is asking for the information – are they who they say they are?

1.4 Whenever a request for information is received you need to be certain of the identity of the requester. You should always verify the identity of a telephone requester by:

- checking that they are acting with the customer's consent. If in doubt check directly with the customer
- telephoning back on a known number **or**
- insisting that the request be made in writing if there is any doubt about the identity or status of the requester or validity of the request.

1.5 It is important to be aware that bogus callers may attempt to obtain personal information from you. The vast majority of bogus contacts are made by telephone and may be from people working for:

- debt collectors
- tracing agencies
- private detectives or
- the media.

These callers can be very convincing, sometimes working from detailed scripts with a great deal of knowledge about our customers. It is also common for the bogus caller to have a good knowledge of departmental procedures and jargon. They may even have worked for the Department in the past.

1.6 Guidance on verifying identity and dealing with bogus telephone calls and reporting bogus calls can be found on the Security Intranet site (Bogus Calls – Guidance).

Standard report forms are also available on this site. Using these forms will ensure that all the necessary information is recorded, provided they are completed fully and.

Further information on representatives and establishing identity can be found at Appendix 3.

Can you establish that consent has been provided?

1.7 Once the identity of the requester has been established, the question of consent also needs to be considered if the requester is not the customer him or herself. Personal information cannot normally be disclosed without the consent of the customer, however general information may e.g. what type of benefit to claim, what claim form needs to be completed.

1.8 Consent from a customer can be made in writing, verbally or it may be implicit. Written consent from the customer must always be requested if you cannot establish verbal or implicit consent. The information may be needed because the customer has urgent needs or problems to address or there are communication barriers such as language or other difficulties in understanding information.

Implicit consent

1.9 Implicit consent applies when, for example, you are dealing with a known and bone fide person or organisation such as Members of Parliament (MP), Members of Scottish Parliament (MSPs), Citizens Advice Bureaux (CABx) etc. Further guidance on these issues can be found in Appendix 3. In such cases it should usually be obvious that the customer has sought the assistance of the representative. However do not be complacent and if you have any doubts at all seek further advice.

If consent is not provided can you still disclose?

1.10 If consent is not provided, disclosure may still be appropriate if:

- a court order is produced. This can still be challenged if you feel that releasing the information would be harmful or dangerous for example where the customer is living at a “safe address”. In such cases you must seek further advice from your local Area Legal Office, ACI INF (DP/FoI) or, in Scotland, ACIS or the appropriate Child Support Agency contact

- disclosure would be in the public interest - for example where disclosure is to be made to the police in respect of criminal activity (further information about the public interest is at Part 1 paragraph 7 and Appendix 2 gives guidance on disclosures to the police)

- there is a Departmental interest

- to prevent duplication of payment from public funds where a specific statutory gateway exists

- it is required by statute **or**

- the customer has a valid representative (see Appendix 3).

Relevance of Information

1.11 When considering a decision to disclose personal information, you need to be satisfied that the requested information:

- is necessary and relevant to the enquiry **and**
- cannot be obtained more appropriately elsewhere, for example another government department or LA asking for information that they may have access to in their own organisation or information being sought that is better coming from a GP or bank.

1.12 Your response must be limited to providing **only** that information which is absolutely necessary, and no more, to deal with the specific issue. You should ensure that:

- only factual, relevant information is given
- you do not give any medical information, refer the requester to the customer
- you do not generally give any information about a criminal conviction
- you do not give any personal opinions.

1.13 **Ultimately it is the responsibility of the officer disclosing the information to ensure that the requester is who they say they are, and that it is appropriate to pass on the information requested. Staff should always take reasonable steps to be satisfied that the enquirer is genuine, that the customer consents, and that the information to be disclosed is relevant.**

2. Grading of decision maker

2.1 It is possible that officers of any grade may be required to make a decision on disclosure and it is therefore difficult to specify this level. For example, there may well be operational reasons for handling requests at certain grades. There are however specific areas where the grade of the decision maker is prescribed, for example disclosures to the police (see Appendix 2 paragraph 6).

2.2 Additionally, consideration needs to be given to the particular sensitivities of the information being requested i.e. the more sensitive the information the greater the need to apply judgement and the need for the decision to be made at a higher grade. If there is any doubt about this please contact ACI INF (DP/FoI) for further advice.

3. Proactive disclosures

3.1 There may be circumstances where it is appropriate to make a disclosure to, for example Social Services, Social Work Department in Scotland or similar organisations without a request being made to you. Such proactive disclosures will usually be in circumstances where there is an urgent need to protect the public or an individual, for example if it is necessary to prevent injury or damage to the health of the customer.

3.2 In such a situation you must first seek advice from your line manager or other senior officer who should seek further advice/clarification from DDPU if there is any doubt about making the disclosure. It is important to record the reasoning behind the decision in case you are later required to justify the disclosure. **See Appendix 2 (paragraphs 15.1-15.2) for more information on proactive disclosures to the police**.

4. Vulnerable persons

4.1 If there are indicators to suggest that a child or vulnerable person is at risk of injury, ill treatment or neglect, you may volunteer the information to Social Services, Social Work Department in Scotland or the police if appropriate. The information given should be factual. Information may be provided without the consent of the parents if a child's welfare is at risk. Always seek advice and permission as per Appendix 2 (paragraphs 15.1-15.2) if you are considering a proactive disclosure.

5. Deceased persons

5.1 The Data Protection Act does not apply to deceased persons, but the rules of confidentiality continue to apply. Generally, if someone enquires about a deceased person you may disclose the date of death only (providing this has already been verified) – do not provide any other information. For further information see Appendix 4 (paragraphs 10.1-10.9).

6. Recording your decision

6.1 **It is important that a written record is kept of any information given. This is to enable you to refer back to an audit trail if any queries arise, and is for your own protection should any dispute arise over the information disclosed.**

7. Where to go for advice

Roles and responsibilities of ACI INF (DP/FoI), ACIS and ACI INF (DDPU)

7.1 **ACI INF (DP/FOI)** is the Department's policy focal point on the application of DPA and FoI legislation, including the interaction with Social Security legislation, as well as the operation of the Open Government (OG) Code.

7.2 ACI INF (DP/FoI) provide overarching advice and guidance to ACI INF colleagues in DDPU, ACIS and other areas. ACI INF (DP/FoI) also offer help, advice and guidance to anyone working on the development of new polices and procedures, especially those which involve the collection, processing or storage of customer or staff information (either electronically or clerically), claim forms, or non-fraud related data-sharing.

7.3 **ACI INF (DDPU)** provide advice and guidance at an operational level for field staff on Data Protection, disclosure and confidentiality issues. DDPU will generally be the first port of call, following local escalation as necessary, for enquiries relating to requests for personal information. DDPU are also responsible for advice on the Subject Access Request (SAR) process within the Department.

7.4 **ACIS** provide advice to DWP staff in Scotland on the impact of Scottish Law on policy and procedures. They also provide advice in Scotland on disclosure of information issues.

7.5 If you are in any doubt about disclosure you should always ask for further advice, firstly from your line manager. If a decision cannot be reached or there is concern about any aspect of the enquiry you should, in the first instance, contact the officer or section nominated with responsibility for such issues within your business unit, for example

within CSA this will be the Monitoring and Guidance Unit (MAGU). Further advice can be obtained from DDPU, ACI INF (DP/FoI) and ACIS.

7.6 **Contact details**

Departmental Data Protection Unit (DDPU)
Room BP 6002
Benton Park View
Newcastle upon Tyne
NE 98 1YX
Telephone: 0191 225 5291
0191 225 3154
Fax: 0191 224 7472
E-mail: Data Protection CCP General

Adjudication and Constitutional Issues Data Protection and Freedom of Information (ACI INF (DP/FoI))
2nd Floor, Adelphi
Telephone: 020 7962 8581
020 7962 8633
020 7712 2418
020 7712 2820
Fax: 020 7962 8725

Adjudication and Constitutional Issues Scotland (ACIS)
Room D311
Argyle House
Lady Lawson Street
Edinburgh
EH3 9SH
Telephone: 0131 222 5657
0131 222 5631

Fraud Strategy Unit
Professional Standards Unit
Counter Fraud Investigations Division
Jobcentre plus
Department for Work and Pensions
Fifth floor West
Trevelyan Square
Leeds
LS1 2ED
Telephone: 0113 2327005

Matching Intelligence and Data Analysis Service (MIDAS)

Room D402
Moorlands Road
Lytham St Annes
FY8 377
Telephone: 01253 334444

Monitoring and Guidance Unit (CSA)
Block C309
Lytham St Annes
Telephone: 01253 339982; or
01253 339971; or
01253 339843
Fax: 01253 339927; or
01253 339949

APPENDIX 1

LOCAL AUTHORITIES

1. Introduction

1.1 This section gives guidance on:

- the circumstances in which the Social Security Administration Act allows you to give information for Housing Benefit (HB) and Council Tax Benefit (CTB) purposes
- the circumstances when you can give information to Social Services (in Scotland Social Work Departments) and
- other circumstances when information may be disclosed to local authorities

2. Data sharing powers

2.1 DWP and local authorities are constantly developing data sharing powers to enable the modern seamless delivery of Benefits and Services to the public. As new initiatives are developed new legal gateways are being established. Always check the latest position on the ACI INF (DP/FoI) Intranet site. Where local initiatives are being considered you must ensure that any data sharing is permitted under legislation and policy (see Statutory Powers for Data Sharing and Data sharing of Personal Information).

2.2 Many routine forms of data sharing will be covered in specific Business Unit operational guidance.

2.3 **Contact ACI INF (DP/FoI) if any new initiative involves the sharing of personal customer information**.

3. Information required for HB/CTB administration

3.1 The Social Security Administration (Fraud) Act 1997 [SSAFA] inserted several sections into the Social Security Administration Act 1992 [SSAA]. Section 122C of the SSAA, permits the disclosure of certain information required for HB/CTB administration to local authorities for HB or CTB.

3.2 Section 122C(2) provides that information may be supplied to:

- an authority administering housing benefit or council tax benefit or
- a person authorised to exercise any function of such an authority relating to such a benefit, for use in the administration of such a benefit

for use in the administration of such a benefit. This information is normally available to local authorities on a Remote Access Terminal (RAT). Where Local Authorities request information from DWP and that information is not already available to them under the RAT system, DWP can release that information to the LA as set out in Section 122C.

The term ‘administration‘ in this context includes:

- calculation of entitlement to benefit
- checking the accuracy of HB/CTB
- calculation and recovery of overpayments
- preventing, detecting, investigating or prosecuting HB/CTB fraud Administration.

3.3 **Information acquired under section 122 or 122B of the Social Security Administration Act 1992** (i.e. information from Inland Revenue or information obtained from government departments relating to passports, immigration and emigration, nationality or prisoners), may **only** be supplied:

- for use in the prevention, detection, investigation or prosecution of offences relating to housing benefit or council tax benefit: **or**
- for use in checking the accuracy of information relating to housing benefit or to council tax benefit and (where appropriate) amending or supplementing such information.

4. Services contracted out by local authorities

4.1 Many LAs have contracted out various services relating to the administration of HB/CTB. Where this is the case, information can be disclosed to the contractor in the same way as to the local authority itself. However, you must still satisfy yourself that all the criteria in paragraph 3 are met.

5. Social Services (Social Work Department in Scotland)

5.1 When to disclose information

Information should only be disclosed if:

- the person concerned has provided their consent
- the person concerned is a danger to themselves or others, or a child or adult is at risk of injury, ill-treatment or neglect (see Part 2 paras 3.1 & 4.1; Appendix 2 paras 14.1 to 14.4 and Appendix 4 para 3.6)
- there is a Court Order requiring the information to be disclosed; or
- the Social Services Department (or in Scotland, the Social Work Department) are legally empowered to receive the information, i.e. Power of Attorney (see Appendix 4 on Representatives for further information).

6. People receiving local authority care or help

6.1 LAs are now required to introduce fairer charging policies for home care and other non-residential social services, sometimes shortened to "Fairer Charging". LAs need to confirm whether Attendance Allowance/Disability Living Allowance (AA/DLA) is in payment. This is done with customer consent. DLA/AA Bulletin 07/03 provides guidance on when information can be disclosed.

If the LA needs confirmation of any other DWP benefit for any other purpose the consent of the customer **must** be obtained.

7. Fraudulently obtained benefits or services

7.1 LAs can prosecute persons who have fraudulently obtained a service or LA administered benefit. Confirmatory statements, documents and information can only be disclosed in these circumstances and only where it is directly related to the investigation or prosecution of local authority administered benefits or services.

APPENDIX 2

THE POLICE

1. Introduction

1.1 All requests from the police should be handled in accordance with the policies outlined in various Memoranda of Understanding (MoU). The Memoranda are between DWP and the Association of Chief Police Officers (ACPO) and the Association of Chief Police Officers in Scotland (ACPOS) and can be found on the ACI INF (DP/FoI) Intranet site; see MOU - England, Wales and Northern Ireland and MOU - Scotland

(See paragraphs 17.1 to 17.5 for information on the Memoranda in respect of registered sex offenders).

1.2 The Memoranda ensure effective co-operation by promoting a clearer understanding of DWP policy in relation to disclosure of information. They provide the overarching policy guidelines to support DWP and police co-operation at an operational level.

1.3 A major driving force behind the memoranda was to put disclosures to the police on a more formal and accountable footing. All requests for information from the police must follow the criteria laid down in the Memoranda. In particular, **requests must be in writing and on the agreed request form at Appendix 1 of the Memoranda. It is not acceptable to provide information to the police or indeed anyone else, in response to a verbal request whether this is over the telephone or face to face.**

1.4 **If any pressure is brought to bear by the police to release information not in accordance with MoU criteria, please contact ACI INF (DP/FoI) immediately.**

1.5 In addition to the over-arching policy Memoranda mentioned at paragraph 1.1, there is also an agreement which sets out the operational protocols to be used in tackling benefit fraud in England and Wales. This agreement covers operational co-operation between the Police and DWP in investigating DWP fraud and is titled “Memorandum of Understanding between the Department for Work and Pensions’ Counter-Fraud Investigation Division and the Association of Chief Police Officers for Operational Support and Investigation Co-operation”. **To avoid confusion with the departmental policy Memoranda the operational agreement is to be known as the CFID Agreement**. The Agreement can be found by clicking: CFID Agreement.
Fraud staff seeking advice on the CFID agreement should approach the Professional Standards Unit. Contact details can be found at Part 2 paragraph 7.6.

1.6 The police may ask for information for a number of reasons for example, information on suspects or when trying to contact witnesses to, or victims of, crime. It may not always be appropriate to disclose the information, for instance you cannot normally disclose information relating to lists of individuals; only in respect of named individuals as we have a duty to maintain the confidence in which customers provide the Department with information. See paragraph 8 for more information on lists of individuals. Additionally, greater consideration needs to be given to requests in respect of witnesses or victims. It will always be necessary therefore to consider each request very carefully before any information is given to the police.

1.7 Requests from bodies such as Air Force, Naval or Military Police, Transport Police,

Procurators Fiscal or specialised units such as Special Branch or the National Crime Intelligence Service etc should be treated in exactly the same way as requests from the police. Whilst they may not be individual signatories to the Memoranda the underlying principles, particularly in relation to compliance with Data Protection legislation and Departmental policy, equally apply.

1.8 The criteria required on the Appendix 1 request form of the Memoranda represent the **minimum** information necessary to inform our decision-making. To enable us to make a fully informed decision, more information may be required than that originally supplied by the police. Do not worry about asking the police for more information; the more information we have the better informed and justifiable our decision will be and this can only be beneficial to the Department and the police.

1.9 It is important that the police are aware of the limitations of our ability to effectively conduct searches. In all probability, we can be reasonably confident of addresses in respect of benefit recipients but not of non-benefit customers/clients. ACI INF (DP/FoI), through the Home Office, ensure that police forces are aware of this limitation.

2. General Policy

2.1 DWP takes a very positive approach to providing information or, where appropriate, documentation, to police forces and other law enforcement bodies, to assist in the prevention and detection of crime and the apprehension and prosecution of offenders. Such disclosures are permissible under section 29(3) of the DPA. However in such cases it must also be shown that failure to disclose the information would significantly prejudice the police investigation.

2.2 The general principle is that DWP will be as helpful as possible whilst maintaining a respect for the confidentiality of the personal information we hold about our customers.

2.3 **Without a court order or customer consent, it will always be up to the discretion of the DWP whether they feel that the public interest argument in favour of disclosure has been adequately addressed in the information provided by the police to support their request.**

2.4 In addition to providing information, in accordance with the Memoranda, to assist in the prevention and detection of crime and the apprehension and prosecution of offenders, information may also be disclosed to the police where:

- disclosure is required by a court order **or**
- the customer consents to the disclosure **or**
- where it is required or permitted by statute **or**
- the Department has a particular interest in the offence in question e.g. benefit manipulation and fraud (in such cases in England and Wales refer to the operational CFID agreement covering the relationship between the police and the Department in the investigation of benefit fraud[1] - see paragraph 1.5)

[1] "Memorandum of Understanding between the Department for Work and Pensions' Counter-Fraud Investigation Division and the Association of Chief Police Officers for Operational Support and Investigation Co-operation"

3. Non-Routine Disclosures

3.1 Information is not routinely given about:

- groups of customers e.g. all males in an area between certain ages i.e. lists (see paragraph 8)
- a person's medical condition
- documents which originated from other government departments or for example the NHS, (or information derived from such documents), **that have not been used to update our records**. However, as the majority of documents from other departments will have been used for this purpose there will, in practice, be little information that falls into this category. If it does, inform the police that they will have to approach the relevant department for access to this information
- benefit details – it is usually unlikely that failure to disclose benefit information would be likely to prejudice an investigation
- It would also be unlikely that complete files e.g. Case Papers, GBUs or files would be released, however extracts or individual documents **may** be released depending on the circumstances of the individual request or case.

In such situations guidance should always be sought from ACI INF (DP/FoI).

4. Matters in which the Department has an interest

4.1 The following list is indicative of matters and offences in which DWP has an interest, but it is not exhaustive:

- fraud or attempted fraud, against the Department
- assaults on DWP staff
- burglary at, or malicious damage to, DWP offices (including receipt of threatening letters or suspected letter bombs)
- trespassing or obstruction on DWP premises
- impersonation of a DWP officer
- unauthorised possession of DWP documents
- misuse or theft of benefit by a third party, e.g. an appointee fails to pay the fees at a residential home in which the customer lives
- failure to pay a fine or cost ordered to be paid to DWP, as a result of a conviction for an offence against the Department
- internal fraud or financial irregularity perpetrated by DWP staff .

4.2 Information should only be given to the police about these offences in a signed written statement (the customer's written consent is not required). Supporting documents (claim forms, encashed giros/order book stubs etc.) and statements can also be provided if these are necessary for the prosecution of the offence. The operational CFID Agreement gives further details (see paragraph 1.5).

Handling requests under the Memorandum of Understanding

5. Who handles Police requests

5.1 Within Jobcentre plus, requests for basic address information are handled by Operational Intelligence Units (OIUs). The only other disclosure activity OIUs should be engaged in is in relation to investigating fraud or responding to requests for information for which CFIS are the primary unit with responsibility for the information.

5.2 Requests for information from other bodies such as CABx, solicitors, MPs, MSPs etc which are not fraud related, or for which CFIS do not have primary responsibility, must be handled by the appropriate business unit as part of the department's normal business and not by OIUs.

5.3 **Information concerning attendance at local Jobcentre plus offices, possibly leading to police attendance at that office, must be handled by the relevant office manager**.

5.4 Witness statements are often required to verify information obtained from departmental computer systems. Therefore information about benefit entitlement and receipt is applicable to the relevant benefit office and **not** OIUs.

6. DWP Decision makers

6.1 The police will indicate on the Appendix 1 request form from the Memoranda whether the offence under investigation attracts a non-imprisonable or imprisonable sentence. This is an important factor in determining the grade of DWP officer who will consider a decision to release information.

6.2 If there is any doubt as to which of these two categories the request falls into, the procedures appropriate to non-imprisonable offences will apply i.e. the request will be handled by an officer of at least Higher Executive Officer (HEO) grade.

Non-imprisonable offences

6.3 **An officer of at least HEO grade** will make decisions in these cases. Judgement will need to be applied as to whether release of the information is in the public interest. The public interest cannot be universally defined as the individual circumstances of each case must considered. However in essence we need to assess whether in each case there is sufficient justification to break any duty of confidence that we owe our customers. In case of any doubt about the application of the public interest test please contact ACI INF (DP/FoI).

Imprisonable offences

6.4 **An officer of at least Executive Officer (EO) grade** will make decisions in these cases. For requests for basic information such as an address, it is very unlikely that a request would be refused as long as the Appendix 1 request form is fully and correctly

completed giving enough detail to enable an informed decision to be made.

6.5 **If the request is for more than address details or for sensitive information a more senior officer of at least HEO grade must be consulted on the merits of the request**. Sensitive information could include medical, financial or gender issues – these examples are not exhaustive.

Complaints or challenges by a customer

6.6 In the event that a customer questions or challenges the police force about DWP passing information to the force, the relevant police force should contact the DWP officer who responded to the original request. The DWP officer will consider whether the correct procedures have been followed and respond as appropriate. In case of any doubt further advice should be sought from ACI INF (DP/FoI).

7. DWP Review of decisions

7.1 If a police officer wishes to query a DWP decision, either because insufficient or indeed no information is provided in response to a request, contact should be made with the DWP officer who made that decision. A more senior officer will then review the original decision. The reviewing officer will consider any additional information supplied by the police in support of the re-submission of the request and will also assess whether all relevant factors were taken into account in reaching the original decision.

8. Requests for information on lists of customers

8.1 DWP will not normally provide police forces with information on lists of customers. However it is accepted that in certain circumstances police forces may believe that a list of suspects is the only manner in which an investigation may be furthered. **Decisions on the release of information relating to a range of persons must not be handled at a local level - these will be considered by ACI INF (DP/FoI) or ACIS who will provide advice on how to handle the request. If it is considered appropriate for assistance to be given this will fall to the relevant local business unit at the direction of**
ACI INF (DP/FoI) or ACIS.

8.2 If information about a number of individuals is necessary to an investigation, police forces must narrow down any list of individuals before submitting it to the Department. DWP would need to have any list reduced wherever possible, to the minimum number of clearly identifiable suspects needed to further the investigation. It is for the police, and not DWP, to take appropriate steps to ensure that a list of suspects is sufficiently narrowed for DWP to consider assistance.

8.3 For example, if the police ask for a list of all customers in a particular area of a certain age, this would be too widely drawn. However, if by providing further information, which significantly reduces the search criteria and better targets the request, help will be considered.

9. Witnesses or victims

9.1 There is no underlying policy or legal reason why assistance cannot be given to the police in the tracing of witnesses or victims of crime. The exemption to the DPA principle of non-disclosure which refers to the prevention/detection of crime and the apprehension or prosecution of offenders does not distinguish between the suspect/offender and a victim or potential witness. Indeed, failure to disclose may in itself prejudice the investigation or prosecution. Each request must be considered on its own merits and careful consideration given (at HEO level) to assessing whether the public interest is being served by a disclosure of a particular piece of information.

9.2 For further information or guidance on specific individual requests please contact ACI INF (DP/FoI). For advice and guidance on handling specific requests from Scottish Police forces please contact ACIS (see paragraph 18.3).

10. Criminal Cases Review Commission

10.1 You may receive requests from the police in respect of investigations on behalf of the Criminal Cases Review Commission or the Scottish Criminal Cases Review Commission or indeed directly from the Commissions.

10.2 The Commissions are independent bodies established to consider cases where it is alleged that a miscarriage of criminal justice has occurred. Their principle role is to review the convictions of those who believe they have either been wrongly found guilty of a criminal offence, or wrongly sentenced.

10.3 In such cases there is a strong public interest argument which justifies disclosure. It is unlikely therefore that assistance will not be given. Such requests must be considered by, at least, HEO grade. If you receive such a request please consult ACI INF (DP/FoI) or ACIS.

11. Written statements

General

11.1 The police will sometimes ask for written statements. It must be remembered that a DWP officer who gives a statement may be required to attend court at a later date.

11.2 The police usually need information to progress an investigation, rather than for use as evidence. If, however, a statement is required in a case where there is no DWP interest, one can only be provided where:

- disclosure is in the substantial public interest **and**
- the information is factual and relevant **and**
- it is not available from another source.

11.3 When a statement is given, the DWP officer concerned must write or dictate the statement him/herself and take into consideration the following:

- only include factual, relevant information
- include references to conversations with the accused or the suspect only

- always keep a copy of any statement given **and**
- consult with Area Legal Office (or in Scotland, ACIS) if queries arise about what could or should be included; **also**
- line management must be informed.

11.4 If a statement is being provided in connection with something that a DWP member of staff has witnessed, the staff member involved must make the statement in a personal capacity. If, however, the police are requesting general details about a case it may be more appropriate for a section supervisor or manager to make the statement should the need arise in future to attend court.

12. Proceeds of Crime Act 2002

12.1 Under the Proceeds of Crime Act 2002, the police may ask for information because they are trying to establish the legitimate income of a convicted person. This will be because they need to prove that income is mainly derived from criminal activity (e.g. income from drugs) and under these circumstances a Court Order must be produced before information can be disclosed.

12.2 Police officers will often ask DWP to check an individual's benefit position **before** they apply for the Court Order in order to see whether it is worthwhile making the application. Accessing our customer's records in such cases is not acceptable and the police must be told that they must follow the provisions of the Proceeds of Crime Act.

12.3 As the purpose is to ascertain a person's legitimate income it is in the individuals own interest to provide the police with consent to approach the Department for information and receipt.

13. Requests for documentary evidence

Departmental interest

13.1 Documentary evidence can be released in cases in which DWP has an interest (also see paragraph 1.4 about the operational CFID Agreement). A receipt must be obtained from the police clearly identifying each document loaned to them. Unless the document is required for forensic purposes (e.g. testing for fingerprints) you must give the police a photocopy. If an original document is required by the police, ascertain why the original is required and if satisfied with their reply, obtain a receipt detailing exactly what information has been given and keep a photocopy of all documents.

13.2 **It is for the 'information owners' to make any decision on such requests** e.g. it is not appropriate for the OIU to decide on release of documents held by a benefit office if the police investigation is not DWP fraud related.

Substantial public interest

13.3 Documentary evidence must only be released to the police in the event of a serious crime where there is a substantial public interest argument in release if:

- you are certain it is relevant to their investigation
- it is essential to their investigation **and**
- there is no other source from which to obtain the information.

13.4 If the police are investigating a serious crime and ask for an original document you will need to obtain an undertaking from the police, which must be signed by both the office manager who has responsibility for that particular information within the department, and the police. The original document must be given to the police along with the undertaking but remember to make copies of the undertaking and all documents loaned.

13.5 The undertaking makes it clear that any documents (whether original or copied) loaned by DWP are for the purpose of the police investigation and any subsequent court case only and must not be passed on to anyone else without permission from the Department. Do not give permission for the document to be used:

- for any purpose other than the investigation **or**
- as information to be passed on to another individual or body.

14. Missing/vulnerable persons

14.1 Departmental policy, and supporting guidance, acknowledges there are situations where it would be appropriate to assist in the tracing of a missing person. However, it is also accepted that it is a person's right to go missing from family and friends. Indeed there may be very good reasons for them doing so and not telling anybody where they have gone. **But** if there is evidence that the person is a danger to themselves or to others, or if there is any evidence of vulnerability or risk, then disclosure may be appropriate.

14.2 Each case must be assessed on its own merits and careful consideration must be given to the specific circumstances behind the request. In particular, it will be appropriate to consider the age of the missing person, all the circumstances surrounding their disappearance, any mitigating medical information whether it relates to physical or medical health and the possibility of potential harm either to themselves or others.

14.3 This principle equally applies to proactive disclosures to local authority social services in respect of vulnerable people where there are indications to suggest that the individual is at risk of ill treatment or neglect.

14.4 **In order to assess the criteria outlined above it is appropriate for such requests to be handled by local management at the benefit/Jobcentre plus office and not within the OIU.** Again, guidance should be sought from ACI INF (DP/FoI) or ACIS.

15. Volunteering information

15.1 There may be information in DWP records, or known to an officer in their official position, which could help the police to investigate an offence and therefore potentially justifies a proactive disclosure to the police. Alternatively you may be aware of a customer who may be a threat to public safety, and/or is placing members of the public in immediate danger. Information may be volunteered **only with the authority of a senior officer from your office**.

15.2 An oft-quoted example of such a proactive disclosure is where a member of staff recognises someone on BBC's Crime watch programme. A degree of common sense needs to be applied here. Generally speaking it would be better to wait until your return to work and to discuss the matter with a line manager/senior officer. However, if the crime being reported is so serious, or there is a particular and immediate danger to members of the public, and the member of staff feels that an immediate approach should be made to the police, or the programme itself, then it may be reasonable to make such an approach. **In such a situation the staff member must speak to their line manager/senior officer at the earliest opportunity and record the reasoning behind the decision.**

16. Letter forwarding

16.1 It would be very unlikely that DWP would forward a letter on behalf of the police. If you receive such a request please contact ACI INF (DP/FoI). Further guidance on letter forwarding can be found in Appendix 4 (paragraphs 3.1 – 4.3)

17. Registered sex offenders

Memorandum of Understanding [MoU] - Location of Sex Offenders

17.1 This section refers to the tracing of registered sex offenders who have failed to meet the registration requirements under the Sex Offenders Act 1997 and not to the investigation of sexual offences such as rape, indecent assault etc which are handled in accordance with the overarching Memoranda and the previous paragraphs of this Appendix.

17.2 The Sex Offenders Act 1997 requires certain sex offenders to register with the police. The vast majority of offenders who have a requirement to register do so. However, a small number of offenders fail to comply with their registration requirements and thereby deny the police the opportunity to analyse and assess those individuals who may represent the greatest risk to the community. By assisting in locating those offenders who fail to register with the police, or who exploit the legislation, DWP can make a valuable contribution to the protection of the public from sex offenders.

17.3 DWP have agreed Memoranda with ACPO and ACPOS covering disclosures in respect of sex offenders and they must be adhered to in all cases.

17.4 The purpose of the Memoranda is to:

- ensure effective lines of communication so that the DWP knows what it may or may not do as regards sharing information and further disclosure, so that it does

not exceed its powers under the law

- provide guidelines to assist police and DWP co-operation at an operational level and
- encourage the exchange of information with the objective of establishing the location of those persons who have a sex offender registration requirement or who present a further risk of harm to the public.

17.5 The Memoranda ensure that:

- disclosures are lawful
- the required test of substantial public interest is met and
- we do not put the safety of individuals at risk

Copies of the Memoranda can be found here:
MOU - Sex Offenders (England, Wales) and MOU - Sex Offenders (Scotland) .

18. Contact details

18.1 Due to the particularly sensitive nature of these cases the processing of the information will always be carried out in a secure environment on a strictly need to know basis. All requests under the Memoranda will be handled by the contacts below and must not be actioned at local level. It is important that we do not put our staff in a difficult position with regard to having knowledge of the sexual offences of customers and the whereabouts of sex offenders.

18.2 All requests under the “Memorandum of Understanding - Location of Sex Offenders” in England and Wales must be referred to:

Department for Work and Pensions
Room 3S 25
Quarry House
Leeds LS2 7UA
Tel: 0113 232 4045

18.3 **Enquiries relating to the "Memorandum of Understanding - Location of Sex Offenders" in Scotland must be directed to**:

Adjudication and Constitutional Issues Scotland
Room E417, Argyle House
3 Lady Lawson Street
Edinburgh EH3 9SH
Tel: 0131 222 5657/5629

18.4 **All requests for registered sex offenders’ information should always go to the named contacts above, and not to OIUs or local offices.**

APPENDIX 3

REPRESENTATIVES

1. Introduction

1.1 This section sets out the general principles of dealing with enquiries from representatives. It aims to assist in the decision-making process of whether to disclose information. The aim is to achieve a balance between allowing the customer the right to third party advocacy, and ensuring that personal information is not passed unlawfully into the wrong hands.

1.2 Customers have the right to enlist the help of an advice or welfare organisation. The Department must respect that right and co-operate with organisations where possible. Effective communication with recognised advice or welfare organisations is both necessary and in our customers' interests. It is important that organisations feel confident in contacting an office for help with customer's problems. However, written consent from the customer must always be requested if verbal or implicit consent cannot be established.

1.3 A customer's representative is any person or organisation acting on behalf of, or making enquiries for, the customer. Representatives may be individuals, such as relatives, social workers, doctors, MPs, or advice or welfare organisation staff, such as CAB, Social Services Welfare Rights Unit (or a Social Work Department Welfare Rights unit in Scotland) etc or independent advice centre.

1.4 Representatives should only be given information when they are acting on behalf of, and with the consent of, the customer. Requests for information may be for many reasons and **each should be considered on an individual basis**.

1.5 Child Support legislation has a specific regulation covering representatives and when staff need to obtain written consent. Further information on CSA representatives can be found in the CSA business specific disclosure guide.

2. Initial steps

2.1 There are three clear steps to be taken before disclosing information to representatives. You must be satisfied that:

- the representative is who they say they are (see paragraph 3) **and**
- the representative is genuinely acting with the consent of the customer (see paragraph 4) **and**
- the information requested is appropriate and relevant to the enquiry (see paragraph 6).

2.2 **If you are in any doubt** about whether the representative is who they say they are, whether they are acting with the customer's consent, or whether the information is appropriate and relevant, you should not disclose information. In such cases always seek advice from your line manager or DDPU.

3. Establishing that the representative is who they say they are

3.1 You must always establish that the representative is who they say they are. If the representative is a private individual, or from an organisation which you do not know to be a genuine advice or welfare organisation, you should insist on seeing written authority from the customer before disclosing information. If an enquiry is received from an advice or welfare organisation then do the following:

- if the customer is present, confirm the identity of the representative, and that the customer agrees to the disclosure **or**
- ring back on a known number (either from the office disclosure list, or the telephone directory) **or**
- ask for written authority from the customer if you are in any doubt about the identity of the caller and the customer is not present.

3.2 If you are able to speak to the customer (either directly or through a third party) you should verify their identity by asking for, for example:

- maiden name
- date of marriage
- their last address
- children's dates of birth
- date of birth
- telephone number or
- other identifying factors that may be present in our records for the individual customer.

4. Establishing that a representative is acting with the consent of a customer

4.1 Information should not be disclosed to an enquirer just because they work for an advice or welfare organisation. Organisations should be given personal information only when you are satisfied that they are working with the consent of the customer. Consent can be established in a number of ways:

- directly from the customer if they are present
- by written, signed authority from the customer, whether held in our records, provided or faxed by the representative
- by telephoning the customer to establish consent **or**
- by accepting that there is implicit consent

5. Implicit consent

5.1 When dealing with a known, bone fide advice organisation, judgement about whether they are acting with the customer's consent can often be made by assessing what information they have been given by the customer about a particular claim, and the nature of the information they are requesting.

5.2 For example, where a representative is able to quote details of a particular benefit application and asks for the reasons why a specific decision was made, it will usually be

quite clear that the customer has given them details of the claim and that, therefore, they are acting on the customer's behalf.

5.3 Offices often keep lists of local organisations that are recognised as legitimate advice or welfare organisations. This does not mean that information can be automatically disclosed if a query is received from someone belonging to an organisation on the list. **You must still be satisfied that the caller is who they say they are, that they are acting with the customer's consent and that the information is relevant and not excessive to the enquiry.**

6. Relevance of information

6.1 Once you have established that the person is who they say they are and that they have the consent of the customer, you then need to be satisfied that the requested information:

- is appropriate and relevant to the enquiry being made
- is not something that the customer would reasonably be expected to know themselves (e.g. their address or date of birth).

7. Disclosing information

7.1 Once you are satisfied that the representative is who they say they are, that they are acting with the customer's consent, and that the information is appropriate and relevant, information may be disclosed to the representative. A written record should be retained of:

- what was disclosed
- to whom **and**
- what steps were taken to confirm authenticity of the representative.

8. General

8.1 Ultimately, it is the responsibility of the officer disclosing the information to ensure that the enquirer is who they say they are, and that it is appropriate to pass on the information requested. Staff should always take **reasonable** steps to be satisfied that the enquirer is genuine, that the customer consents, and that the information released is relevant. If you are in reasonable doubt about the bona fides or motives of a representative you should refuse to provide information.

8.2 **Offices should not**:

- apply blanket policies in disclosing to representatives (**i.e. always** insisting on faxed or written authority from the customer). **In all cases a decision must be made on a case by case basis**
- give passwords for customer representatives to use – there can be no guarantee that these are secure and their use may lead to incorrect disclosure
- accept a blanket authority for the representative to act in all matters for an indefinite period - authority to represent the customer will be considered to be of finite duration or for a particular item of business, for example, from the making

of a benefit claim until the end of the dispute process;

- disclose information indirectly - if in doubt about disclosing, think about what you say – e.g. "I can't give you the information as we don't have a customer of that name" – although you have refused the actual request you may still have given them information that may be useful to them.

8.3 Sometimes information is disclosed to the customer's representative rather than the customer themselves. This may be because the customer has difficulty communicating; customers who do not speak English, for example, may always need a representative to act on their behalf. In a case such as this, if the customer is present in the office with their representative and gives their consent, disclosure will normally be appropriate.

9. Persons legally empowered

9.1 There will be certain representatives who are legally empowered to act on behalf of a customer:

- an appointee is someone who has been legally appointed by the Department to act on behalf of a customer and who receives any payments for them
- a person given the Power of Attorney (by a court or by the customer themselves) deals with all aspects of the customer's financial affairs.

In these cases, you may disclose any information to the representative that could normally be given to the customer. It is not necessary to seek the consent of the customer.

9.2 Guidance on appointee and power of attorney status is contained in the 'Agents, Appointees, Attorneys and Receivers Guide' (Agents, appointees, attorneys & receivers). If you need further advice about whether a person or organisation is legally empowered to act for the customer, please contact Adjudication and Constitutional Issues DMA, 2nd Floor Adelphi, Telephone: 0207 962 8777.

10. Members of Parliament/Members of Scottish Parliament

10.1 It is a long-standing practice within the Department that it **can be assumed that the constituent's consent has been given when an MP makes an approach to the Department on their behalf**. The Department fully accepts that effective communication with MPs, amongst others, is necessary and in our customer's interests, subject to checks or knowledge of the bona fides of the representative. There has never been any policy intention to prevent efficient and effective working relationships between MPs, their constituents and the Department. Recent failures to adequately assist MPs resulted in them writing to Secretary of State complaining that DWP was being obstructive and impugning the integrity of MPs.

10.2 Generally speaking, when an MP writes to the Department **on behalf of a constituent**, it is safe to assume that the constituent has given consent for the approach to be made; i.e. we have the implied (if not explicit) consent of the constituent. In such circumstances, information about the individual can be passed to the MP in order to respond to a specific enquiry.

10.3 Where someone other than the constituent approaches the MP, for example relatives or friends intervening, perhaps inadvertently against the wishes of the individual concerned, it is acceptable to clarify the situation with the MP and to obtain consent

before answering the enquiry. However, such cases should be rare and guidance must be sought from the DDPU before going back to the MP.

10.4 In the case of constituency workers or Parliamentary Secretaries, an element of common sense must be applied. MPs are unable to personally handle every aspect of a constituent's case. For example it is highly unlikely that the MP personally typed the letter and it is equally unlikely (although possible) that the constituent would believe this to be the case.

10.5 There is little problem in advising a constituency worker of the progress of a particular case. This does not mean however that the constituency worker should necessarily be given detailed confidential information about the constituent unless it is clear that it is both appropriate to do so and preferably with the direct knowledge of the constituent. In response to an MP, Secretary of State stated that implied consent "would not normally be automatically" extended to constituency workers. Again, if there is any doubt please contact DDPU, ACI INF (DP/FoI) or ACIS (see Part 2 paragraph 7.6 for contact details).

APPENDIX 4

MISCELLANEOUS

1. Information requested to assist in the prevention or detection of crime

1.1 The Data Protection Act 1998 (section 29(3)) allows for personal information to be disclosed to a third party where it is required for:

- the prevention or detection of crime, or
- the apprehension or prosecution of offenders

1.2 Whilst this provision is mainly used by DWP in respect of disclosures to the police (see Appendix 2) it is possible that other bodies may approach you quoting section 29 of the DPA.

1.3 It is important to remember that section 29(3) is a permissive power only and that it implies no obligation on DWP to provide the information requested. In order to satisfy ourselves that there is sufficiently strong reason to break our duty of confidentiality to the customer we must be satisfied that failure to provide the information would significantly affect the purposes for which the information is requested. This means that there must be a substantial chance as opposed to a mere risk that the purpose for which the information is requested would be prejudiced.

2. Unacceptable Customer Behaviour markings

2.1 Unacceptable Customer Behaviour (UCB) markings are what used to be known as Potentially Violent (PV) markings. UCB is defined as any act of verbal abuse, threatening behaviour, abusive written correspondence, or an actual or attempted physical assault that causes staff to feel upset, threatened, frightened or physically at risk and is directed at them because of their work in the Department. This also applies to incidents that take place outside the office and sometimes in non-working hours, providing that it can be directly connected to staffs' work in the Department.

2.2 All incidents involving such abuse should be reported. Following consideration of the report and acceptance that there has been unacceptable behaviour, the appropriate marking is put onto departmental systems and clerical documents. If appropriate, customer records are also noted with details of any UCB person in the same household.

Disclosure/exchange of UCB information

2.3 The local Health & Safety Representative is copied into the relevant UCB forms, which are anonymised by removing the personal details of the member of staff. In addition, the forms should also be copied to other business units within the Department **where it is known** that they have contact with the customer. Exceptionally it may be necessary to pass UCB information to bodies outside the Department - see additional UCB guidance here: Unacceptable Customer Behaviour Guidance
The Departmental Central Index, where this is available, or Personal Details Computer System should be used to identify those DWP businesses that require notification.

2.4 Where business units need UCB information that would not normally be automatically forwarded to them as in the previous paragraph, they must request the information as and when required.

2.5 When a customer is classified with a UCB marking and they are to be seen by another business unit e.g. the Appeals Service, the Independent Review Service, a Medical

Board or the Veterans Agency the other business unit must be advised that the customer has been classified as UCB.

UCB lists

2.6 The UCB list is a control measure that should be made available to both visiting staff and front line staff, to ensure their safety. The list should contain only the name, address and National Insurance number.

2.7 Security measures must be put in place to ensure that the list cannot be accessed by any unauthorised person; e.g. if it is held on a laptop computer by visiting staff it should be password protected.

2.8 The UCB Policy and guidance which includes guidance about the passing of UCB lists to other businesses, both inside and outside DWP, can be found here: Unacceptable Customer Behaviour Guidance

3. Letter forwarding - contacting customers on behalf of third parties

3.1 There are two types of letter forwarding that the department is asked to participate in:

- forwarding of letters in respect of individual customers and
- bulk forwarding of letters to a large number of DWP customers on behalf of organisations such as insurance companies and pension fund administrators

Individual requests

3.2 These can come from a wide range of organisations and individuals and each request must be considered on its own merits. Departmental policy is that **we would not normally agree to forward a letter unless there was a compelling argument to do so**.

3.3 Usually, letter forwarding in itself does not involve a disclosure of personal information (other than perhaps confirming that a letter has actually been forwarded which may be taken by the requester to indicate that we have on-going business with the customer). However, the Department has been criticised for using information given to it for a clearly defined purpose, for other purposes unconnected with the business functions of the Department and without the informed knowledge/consent of the customer.

3.4 It is not possible to give examples of **all** cases where letter forwarding may or may not be appropriate but some of the more common examples are described in paragraphs 3.5 to 3.12.

Benefit to the individual

3.5 There may be circumstances where the issue of a letter may be to the potential benefit of an individual; for example where an insurance company is holding onto unclaimed benefits or an executor wishes to confer the proceeds of a will. In such circumstances we could be criticised both by the individual concerned and outside bodies if we did not assist. Judgement must be applied in each case with as much information as possible being obtained from the requester to assist us in making an informed decision.

Missing persons

3.6 Such requests may come from a police force, social services or relatives of the missing person. The first point to be taken into account is that we all have the right to go missing if we choose to do so, therefore careful consideration must be given to the specific circumstances behind the request. In particular, it will be appropriate to consider the age of the missing person, all the circumstances surrounding their disappearance, any mitigating medical information whether it relates to physical or medical health and the possibility of potential harm either to themselves or others.

3.7 If the police have reason to investigate a particular absence perhaps suspecting foul play, they should consider making their request for assistance under the terms of the Memoranda of Understanding (see Appendix 2 paragraph 14).

3.8 If the request is more welfare-based it should be considered as in the previous paragraph.

3.9 General guidance on handling requests from Social Services departments can be found in Appendix 1 (paragraph 5) of this document.

3.10 Guidance on providing **information** rather than forwarding a letter, in respect of missing persons can be found at Appendix 2 paragraph 14.

Absent fathers (parents) and maintenance cases

3.11 During a Parliamentary Debate on 4 July 1956 the Parliamentary Secretary emphasised the importance of the confidentiality of information supplied to the Department and stated that the policy of non-disclosure would not be changed. However the Parliamentary Secretary confirmed that the Department was prepared to help by forwarding letters from third parties **where a court order for maintenance or an affiliation order has been granted**. The Department (Ministry as was) “has no desire to protect the husband or father who absconds and avoids his responsibilities under a maintenance order”. The statement was made in the context of absent fathers and pursuing or collecting maintenance. In such cases you should obtain a copy of the relevant order.

Matrimonial/family proceedings

3.12 Disclosure of addresses in matrimonial and family proceedings is covered by Practice Directions issued by the High Court. These set out the minimum information that must be supplied to the department before such requests for an address can be considered. The Directions specify that the applicant or his solicitor should be asked by the registrar (district judge) to supply as much as possible of the following information about the person sought:

- National Insurance number
- surname
- forenames in full
- date of birth (or if not known, approximate age)
- last known address, with date when living there
- any other known address(es) with dates
- if the person sought is a war pensioner, his War Pension and service particulars (if known) [NB: war pensioners now fall under the remit of Ministry of Defence]

- exact date of marriage (if appropriate) and names of the spouse

Letter forwarding is therefore not appropriate in such cases as the Department can supply address information. In case of any doubt please contact DDPU as usual.

3.13 The arrangements at 3.12 are concerned with tracing the address of a person against whom proceedings have been brought by another person seeking to obtain or enforce an order for financial provision, either for her/himself or herself or for any children of the former marriage.

The arrangements at 3.12 also cover tracing the whereabouts of a child, or the person with whom the child is said to be, in abduction or custody cases e.g. in which Custody Orders are being sought or enforced. Given these circumstances, we will provide assistance in providing address information. CSA staff should also refer to their own Agency guidance.

Divorce

3.14 It is highly debatable whether the forwarding of letters in divorce cases could be deemed to be beneficial to the addressee. It would not be appropriate for the Department to assist
in the serving of divorce papers.

Refusals to assist

3.15 Letters should **not be forwarded** in the following situations:

- parent seeking an adopted child
- adopted person seeking biological parent
- any one seeking an ex-partner
- assistance in tracing family trees
- debt collectors or tracing agencies
- tracing of individuals for school reunions etc

Assistance to be provided

3.16 In the very limited circumstances in which it is appropriate to forward a letter, the requester should be asked to supply the following:

- full identity details of the intended recipient including name, last known address, date of birth, previous names, NINo etc

- the letter that is to be forwarded in an unsealed envelope

3.17 The letter to be forwarded must be sent unsealed to DWP in order that the contents can be checked to ensure that they are in line with the reason behind the request and that it does not contain any harmful material. It is not necessary to confirm as a matter of course that the letter has actually been despatched; however it would be unlikely that we would refuse to do so if asked to.

3.18 The Department can accept no responsibility for the contents of a forwarded letter and the recipient must be advised of this fact.

4. Bulk Letter Forwarding

4.1 The Compensation Recovery Unit manages a Bulk Letter Forwarding (BLF) operation. This is a service offered mainly to commercial organisations such as Insurance Companies and Financial Institutions that want to forward beneficial information to customers but for whom they do not have a current address. A charge may be made for the service.

4.2 The Unit will not disclose information to the sender about any person, and has the right to refuse applications, or stop processing, at any time. It is up to the person contacted to decide whether to reply to the forwarded correspondence.

4.3 For further information on this service contact

BLFS
Room M0201
Durham House
Washington
Tyne & Wear
NE38 7SF
0191 225 2191/2629/2536

A copy of the Instruction Leaflet for people requesting this service can be found here: Instruction leaflet for BLF

5. Parliamentary Commissioner for Administration (Parliamentary Ombudsman)

5.1 The Parliamentary Commissioner for Administration (the Ombudsman) can ask the Department to provide information about a customer under Section 8(1) of the Parliamentary Commissioner Act 1967. Section 8(3) of the Act overrides DWP's duty of confidence.

5.2 In Scotland the Public Services Ombudsman (set up by the Scottish Public Services Ombudsman Act 2002) investigates Scottish bodies; however she cannot consider complaints about UK government departments such as Department for Work and Pensions and Inland Revenue which fall under the remit of the UK Parliamentary Ombudsman

5.3 The Ombudsman deals with complaints from members of the public that they have suffered injustice because of maladministration by government departments or certain other bodies. She also deals with complaints about problems in obtaining access to official information i.e. non-compliance with Open Government. The Ombudsman is independent of government and is not a civil servant. She is an officer of the House of Commons, appointed by the Queen and reports direct to Parliament.

5.4 The Ombudsman has wide powers to look at an organisation's own papers and record. Her officers can examine the organisation's files and interview its staff. If the information you are asked to supply includes details about a third party, the Ombudsman's attention should be drawn to this fact.

5.5 DWP Viewpoint" has corporate responsibility for managing the Department's relationship with the Parliamentary Ombudsman on behalf of the Permanent Secretary. **It is important that Ombudsman cases receive top priority**.

Further information concerning the process of an Ombudsman investigation can be

found here: The Parliamentary Ombudsman

5.6 Under Section 7 (2) of the Parliamentary Commissioner Act 1967 every investigation by the Ombudsman is conducted in private. Details of enquiries made by the Ombudsman and any replies given by the Department must not be released without first obtaining the permission of the Ombudsman.

6. Personal Injury compensation cases

6.1 All these requests are covered by the Social Security (Recovery of Benefits) Act 1997 and should be sent to Compensation Recovery Unit (CRU). CRU will provide benefit information e.g. rates and date of payment, but may ask a district office to send some background documents such as copy of a claim form.

6.2 DWP is only obliged to provide details of any benefit paid since the accident, injury or disease for "the relevant period" as defined by the Social Security (Recovery of Benefits) Act 1997. In the case of an accident or injury, the relevant period is the period of five years immediately **following** the day on which the accident or injury in question occurred.

6.3 **These requests should not be treated as data protection subject access requests (SARs) even though they may quote the DPA**.

Information to be provided to Compensator/Solicitor acting for Compensator

6.4 These requests should also be sent to CRU as they are also subject to the Social Security (Recovery of Benefits) Act 1997. Details of the incident must be provided by the requesting solicitor and be accompanied by a written authority from the claimant/injured person.

6.5 CRU does not hold any benefit information and will inform the appropriate benefit office, in writing, as to what information may be released. **These requests should not be treated as data protection subject access requests (SARs)** even though they may quote the DPA.

Professional Negligence claims

6.6 In some instances a personal injury case either will not proceed or a solicitor will decide not to take the case forward. In this situation an individual may decide to sue the solicitor for professional negligence. A professional negligence claim may arise in such circumstances due to the loss of opportunity to sue for an appropriate level of damages. These cases are not covered by the meaning of the Social Security (Recovery of Benefits) Act 1997.

6.7 CRU has agreed to handle these requests. This is because the information that may be given in these cases depends on whether a Certificate of Recoverable Benefits, issued by CRU, has already been given.

6.8 CRU will establish what information is appropriate for release, and will then refer back to the appropriate office in order for the relevant information to be obtained and released. **These requests should not be treated as subject access requests (SARs) even though they may quote the DPA**.

Requests should be sent to:

Room M0135B
Durham House
Washington
Tyne & Wear
NE38 7SF
Tel: 0191 22 52643
Fax: 0191 225 2189

7. Motability

7.1 The Motability Scheme is open to people in receipt of the higher rate mobility component (HRMC) of DLA. It enables recipients of this benefit to enter into a contract for hire purchase agreements for cars, powered wheelchairs and pavement scooters.

7.2 The HRMC is paid directly to Motability service providers for the duration of the scheme. Individuals sign a consent form to allow Motability to check that HRMC is in payment via the DLA database and also enables them to check that name and address details are correct. **Motability do not have any authority to check any other information; e.g. any non-dependent details**.

7.3 The Motability Fraud Investigation Unit is not a prosecuting authority therefore requests for any other information from the Unit cannot be made under DPA Section 29(3) - Crime and Taxation and should be refused. There is no other avenue available to Motability.

8. Court proceedings and Court Orders

8.1 The Department is often asked for information for use in court as evidence and staff are sometimes required to attend court on behalf of the Department. **If there is a departmental interest** and you are asked to attend court in your official capacity to give evidence or to produce documents a Court Order, subpoena, citation or customer's consent is not needed.

8.2 **If there is no departmental** interest in the case and unless you have received a subpoena, citation or other court order, you should not in your official capacity;

- attend court **or**
- give evidence **or**
- provide documents for the court

8.3 If you receive a Court Order which asks for the production of documents that do not belong to the Department you should inform the court who owns the documents.

8.4 If you are asked to attend court on behalf of the Department and need further advice you should contact your local Area Legal Office, ACI INF (DP/FoI) or ACIS. A court order may require the attendance of a named individual, perhaps because they have detailed knowledge of the case, or the Secretary of State (i.e. an officer of the Department rather than a named individual). In the latter case, the attendance will be necessary in order to produce documents in court, and possibly to explain their use.

8.5 **Always check with your local Area Legal Office, ACI INF (DP/FoI) or ACIS** as to exactly which documents are required for production in court.

Challenging Court Orders

8.6 When a court order is produced on most occasions it will be appropriate to disclose the information. However, even if a court order has been produced and you still have concerns that the disclosure may be inappropriate, you should contact your Area Legal Office, ACI INF (DP/ FoI) or ACIS in Scotland for advice.

8.7 If the solicitors agree that a court order should be challenged, this decision should be conveyed to the court by the solicitor. This is important because the member of staff could be held in contempt of court for not providing the information, therefore legal support is essential.

Coroners or Procurators Fiscal in Scotland

8.8 Coroners may ask for information about deceased customers. The Procurator Fiscal (PF) is the equivalent in Scotland although the roles are not identical. Coroners and Procurators Fiscal have judicial powers and can be given information providing that it is relevant to their enquiry.

Petition Warrants in Scotland

8.9 In Scotland, Procurators Fiscal (PF) may request offices to produce documentation where criminal proceedings are being taken against a DWP customer. Where DWP does not have an interest in the case, a citation or court order (petition warrant in Scotland) must be produced before the office complies with such a request.

8.10 An agreement exists between the Crown Office and the Department stating that the request should be received from the PF in an agreed format. When this letter is received by an office, it can be accepted that a petition warrant exists. It is not necessary for the office to insist on sight of it. For further guidance, please contact ACIS.

Legal Services Commission (LSC)

8.11 In order to obtain Legal Aid, the onus of proof of income lies with the applicant. Disclosure of DWP customer information to LSC requires informed and explicit customer consent. If LSA request details of benefits entitlement quoting section 29(3) of the DPA it would be unlikely that disclosure would be made (see section 1 of this appendix).

9. Disclosing medical information to the customer

9.1 Whilst this document relates to the rules to be followed in providing personal information to a person other than the customer him/herself there are also particular conditions to be applied when considering providing personal medical information directly to the customer.

9.2 The DPA states that certain medical information can be withheld if disclosing the information would be likely to cause **serious** harm to the physical or mental health of the customer (e.g. a malignancy, progressive neurological disease or major mental illness of which the customer is unaware). **The decision on whether to withhold the information from the customer must not be made without first consulting an appropriate health professional** i.e. the professional currently or more recently caring for the customer.

9.3 The Data Protection (Subject Access Modification) (Health) Order 2000, allows DWP to continue its current approach of using its own properly qualified and suitably experienced doctors to make a decision on whether to disclose "sensitive personal data". This will help to reduce any delay in tracing the customers GP and ensure that we meet the 40-day deadline when responding to a Subject Access Request from the customer.

In all cases a decision must be made on an individual basis.

9.4 If you are satisfied **beyond doubt** that the customer has already seen or is otherwise aware of the information, it can be disclosed without the file or papers being seen by a health professional.

Additionally, the file does not need to be seen by a health professional if:

- they have been consulted prior to receiving the request and an opinion obtained in writing that the material does not contain "harmful" information **and**
- that opinion is less than six months old **and**
- there has not been a change in their circumstances.

If you are in any doubt pass the file/records/papers to the relevant medical professional for their advice on whether to disclose or withhold the "harmful" medical information.

10. Deceased persons

10.1 The Data Protection Act does not apply to deceased persons, but the rules of confidentiality continue to apply. Generally, if someone enquires about a deceased person you may disclose the date of death only (providing this has already been verified) – do not provide any other information.

Requests for information from executors and administrators

10.2 If a customer dies, another person may have to sort out their affairs. This may be an executor or a person who has taken out letters of administration. Executors and administrators legally act on behalf of the deceased. Information can be given to them or to solicitors acting on their behalf as though they were asking for information held about themselves.

10.3 If the deceased's will is disputed or it is not clear if the will has been legally signed by the deceased, forensic tests may need to be carried out on the deceased's handwriting. The executor or administrator may request an original document that has been signed by the customer. If a solicitor is acting for the executor or administrator, and has provided a written request, the appropriate document should be provided.

10.4 If a request is received from an executor or administrator, who does not have a solicitor, ask them to provide evidence that they are an executor or administrator. When satisfactory evidence is provided, provide the required information. Refer any cases of doubt to the central contact point.

Requests from people other than executors or administrators

10.5 If someone who is not the executor or the administrator requests information about the deceased, you should first check the file to see if any details are recorded about an executor or administrator before giving any information. If there are, you should:

- ask the enquirer to obtain written consent from the executor or administrator or from solicitors acting on their behalf **and**

- not give any information about the deceased without the written consent from the executor, administrator or solicitor acting on their behalf.

10.6 If there is no executor or administrator, then information can be given to a close relative (or to someone with the written consent of a relative), or to the Treasury Solicitor (Bona Vacantia Division) if there are no surviving relatives. The Scottish equivalent of the Treasury Solicitor is the Lord Advocate, via the Crown Office.

Requests from other people – will disputes

10.7 In the event of a deceased customer's will being disputed, whether by relatives or other third parties, information about the deceased may be requested by the person in question. They should be informed that the information is confidential and cannot be disclosed. Explain that the information can only be given to, or with the written consent of, the executor or administrator.

Deceased estates

10.8 If a person dies intestate (i.e. without leaving a will) and without any known relatives, the estate may be administered by the Treasury Solicitors on behalf of the Crown. In these cases you may be asked to give details of any known surviving relative who may be entitled to a share in the estate. Tell the Treasury Solicitor any relevant information about the relative. Details of benefit paid to the deceased person may also be given, if required.

10.9 If there is an outstanding overpayment or Social Fund loan at the time of death, ask the Treasury Solicitor to inform you of the amount of the estate. Take recovery from the deceased's estate when you have obtained the information.

APPENDIX 5

CRIMINAL OFFENCES RELATING TO THE MISUSE OF PERSONAL DATA

Offences under the Social Security Administration Act 1992 and the Child Support Act 1991

1. Section 123 of the Social Security Administration Act 1992 makes it an offence for anyone who is or has been employed in social security administration to disclose personal information acquired in the course of their employment without lawful authority. Section 50 of the Child Support Act 1991 contains similar offences in respect of Child Support employment and information.

2. A disclosure is made with lawful authority if:

    - it is made by a civil servant in the course of official duty
    - it is made by a contractor who is providing services to the DWP in accordance with instructions given by the DWP
    - it is required by law or a court order **or**
    - it is made with the consent of the customer.

3. An offence under this Section is punishable by a term of up to six months imprisonment and/or a fine.

4. Section 115 of the Act, allows criminal proceedings to be taken against corporate bodies and their directors and officers where:

    - an offence has been committed under the Act **and**
    - it occurred with the consent or connivance of the directors or officers of the corporate body, or because of their neglect.

5. One effect of this Section is that where an unauthorised disclosure has been made by a contractor's staff, proceedings may be taken against the contractor or its directors or officers if it can be shown that the contractor's negligence contributed to the disclosure.

Offences under the Data Protection Act 1998

1. Section 21 of the DPA makes it an offence to process personal data without notifying the Information Commissioner, or to give the Commissioner false or incomplete information about data processing. These offences apply only to data controllers – those with overall responsibility for a data processing operation.

2. Government departments cannot be prosecuted under this Section. (Section 63 of the Act refers.)

3. Section 55 of the Act applies to anyone, including staff or contractors working in government departments.

4. Under Section 55, it is an offence to obtain, disclose or procure the disclosure of personal information, without the authority of the data controller, except in circumstances specifically allowed by law, such as the prevention of crime.

5. It is also an offence under Section 55 to sell personal information that has been obtained illegally, or to offer to sell it.

6. If the Commissioner considers that an offence has been committed under the DPA, the Commissioner may bring a criminal prosecution. Prosecutions under the Data Protection Act may also be brought by or with the consent of the Director of Public Prosecutions. Where the Commissioner has reasonable grounds for suspecting a criminal offence or a breach of principle, an application can be made to a circuit judge for a search warrant to enter and search any premises. In Scotland the Procurator Fiscal can bring the prosecution.

Offences under the Computer Misuse Act 1990

1. Section 1(1) of the Computer Misuse Act makes it a criminal offence for any person to cause a computer to perform a function with intent to secure access to any program or data held in any computer where:

    - the access the person intends to secure is unauthorised **and**

    - the person knows at the time when he or she causes the computer to perform the function that is the case.