

GUIDANCE ON DISCLOSING INFORMATION TO THIRD PARTIES IN ORDER TO PROTECT A CHILD CONSIDERED TO BE AT RISK

<u>Contents</u>	<u>Page No</u>
• Introduction	2
• Disclosing Information with consent – General Protocol for the Sharing of Information	3
• Disclosing Information Without Consent	4
Appendix 1: “Decision to Share Information Without Consent” Form	6
Appendix 2: Legal Guidance for completing the “Decision to Share Information Without Consent “ Form	9

Introduction

Legislation and practice in child protection are underpinned by principles derived from Articles of the United Nations Convention on the Rights of the Child, ratified by the UK Government in 1991. These principles are:

- each child has a right to be treated as an individual;
- each child who can form a view on matters affecting him or her has the right to express those views if he or she so wishes;
- parents should normally be responsible for the upbringing of their children and should share that responsibility;
- **each child has the right to protection from all forms of abuse, neglect or exploitation;**
- so far as is consistent with safeguarding and promoting the child's welfare, public authorities should promote the upbringing of children by their families; and
- any intervention by a public authority in the life of a child must be properly justified and should be supported by services from all relevant agencies working in collaboration.

In order to protect a child considered to be at risk it is possible, and on occasions essential, for information about Service Users to be disclosed by staff. Disclosing information held about a child and his/her family to others must be done in line with applicable laws governing this i.e. the Common Law Duty of Confidentiality, the Data Protection Act 1998 and the Human Rights Act 1998.

Disclosures must be handled carefully as failure to observe the proper procedures could result in the Council being exposed to court action or to enforcement activity under the Data Protection Act 1998 for a breach of the data protection principles, the Human Rights Act 1998 for infringing a service user's right to respect for his/her private and home life, or at common law for breach of confidence. In some circumstances, there is the possibility of personal criminal liability attaching to a member of staff. This must be weighed against the responsibility to act to make sure that a child whose safety or welfare may be at risk is protected from harm.

This document contains guidance for staff in dealing with this sensitive issue and is the guidance referred to in Section 9(c) of the Case Recording Policy.

Disclosing Information with Consent

General Protocol for the Sharing of Information

Where the Council has signed up to a General Protocol then the Council must seek the explicit consent of all individual Service Users or their parents/legal representatives as appropriate, in connection with the sharing of information about them with other Parties to the Protocol.

Obtaining explicit consent will satisfy obligations under the Data Protection Act 1998, the Human Rights Act 1998 and the common law duty of confidentiality.

The term “*explicit consent*” is not defined within legislation, but is taken to mean active consent ie consent in writing or, where this is not possible, verbal consent.

When consent is obtained to share information, such consent should be recorded on the Service User’s case file.

One of the purposes for sharing information, listed in the General Protocol, is “to protect children and young people”. Therefore, if consent is in place, there are no barriers to sharing information for this purpose, when necessary, with the other organisations who have signed the Protocol.

Where a member of staff has concluded, in line with NESCPG Guidelines, that there is a reasonable concern that a child is at risk, then that member of staff should ensure that an audit trail is kept on file to support their concerns before any disclosure is made. Such an audit trail is necessary in order to resist a challenge for an unlawful disclosure of information under the Data Protection Act 1998, the Human Rights Act 1998 or the common law duty of confidentiality.

Disclosing Information without Consent

When contemplating a disclosure of information to the other Parties to the Protocol, where no consent is recorded on the Service User's case file, and to others generally who are not a party to any protocol, a "Decision to Share Information Without Consent" Form (see **Appendix 1**) must be completed.

Completion of the Form will provide an audit trail to demonstrate that due consideration has been given to all the legal factors - the common law duty of confidentiality, the Data Protection Act 1998 and the Human Rights Act 1998.

Such an audit trail is necessary in order to resist a challenge for an unlawful disclosure of information under the Data Protection Act 1998, the Human Rights Act 1998 or the common law duty of confidentiality.

The Form should be completed as follows:

1. Part A of the Form should be completed, with as much information as possible, by the member of staff wishing to make, or approached to make, a disclosure. The Form should then be passed to the Designated Manager to complete Parts B to E.
2. The Designated Manager should refer to the **Legal Guidance** (see **Appendix 2**) to enable them to complete Parts B to D of the Form and decide whether
 - there are statutory grounds for disclosure without consent, and/or any of the conditions in Schedule 2 or (where applicable) Schedule 3 of the Data Protection Act 1998 can be met, [Part B] and
 - any of the qualifications in the Human Rights Act 1998 can be met [Part C] and
 - there is justification for breaching the common law duty of confidentiality [Part D].

If the Designated Manager is in any doubt, they should seek legal advice.

3. The Designated Manager should decide whether information can be shared without consent and complete Part E of the Form accordingly.

If a decision is taken to share information, and this can only happen if the decision can be justified in all Parts (B to D) of the Form, then recipients of the information must be made aware that it has been disclosed without consent. They should then store the information securely and not disclose it further.

4. The Service User, if they have the capacity to understand, must then be informed of the disclosure, unless informing the Service User would prejudice the purpose for which the disclosure was made. Part F of the Form should be completed as appropriate by the member of staff who completed Part A of the form.
5. A copy of the completed Form should be kept in the Service User's case file as well as centrally by the Designated Manager.

FORM

DECISION TO SHARE INFORMATION WITHOUT CONSENT

PART A – Background Details

[To be completed by staff members]

Name of Service User

Consent to share information sought on

Consent not obtained because

service user unwilling to provide consent

OR

service user incapable of making the decision to consent

service user incapable of communicating the decision to consent

service user incapable of understanding the decision to consent

service user incapable of retaining the memory of providing consent

AND

The service user does not have a legally appointed representative.

Information that needs to be disclosed [*insert details*]

.....

.....

To [*insert name, post and organisation*]

.....

because [*provide reasons*]

.....

.....

PART B - Data Protection Act 1998 [To be completed by the Designated Manager]

Do statutory grounds for disclosure exist? Yes/No

If yes, please specify

.....
.....
.....

Applicable Schedule 2 Condition (Sch 2 Data Protection Act 1998):
Para. (insert no.)

AND

If "sensitive" information (see **Legal Guidance** for definition) needs to be disclosed, applicable Schedule 3 Condition (Sch 3 Data Protection Act 1998):
Para. (insert no.)

PART C - Human Rights Act 1998 [To be completed by the Designated Manager]

Would sharing information be in accordance with the Data Protection Act 1998 (Part B above)? Yes/No

Sharing information has a legitimate aim in that it is necessary

- in the interests of national security
- in the interests of public safety
- in the interests of the economic well-being of the country
- for the prevention of disorder or crime
- for the protection of health or morals
- for the protection of the rights and freedoms of others.

Is the disclosure of information necessary in a democratic society? Yes/No

Would disclosure of information be in line with decisions taken for other service users in similar situations? Yes/No

PART D - Duty of Confidentiality [To be completed by the Designated Manager]

Is there a public interest justification for disclosure? Yes/No

If yes, insert details

.....
.....
.....
.....

PART E - Authorisation [To be completed by the Designated Manager]

- Sharing information authorised
- Sharing information not authorised

.....
(Signature)
..... (Post)
..... (Date)

PART F – Notification [To be completed by staff members]

- Disclosure notified to service user
- Disclosure not notified to service user

because.....
.....

..... (Signature)
..... (Post)
..... (Date)

Legal Guidance

**for completing parts B to D of the Form
“Decision to Disclose Information Without Consent”.**

This section is relevant to Part B of the Form

This section contains general information on the requirements of the Data Protection Act 1998, lists the Schedule 2 and Schedule 3 conditions and is then followed by some general scenarios with suggested applicable schedule 2 and schedule 3 paragraphs.

Data Protection Act 1998 – (DPA 1998)

General

Personal information/data about service users is held by the Council. The information covers both facts and opinions about the service users and includes information regarding the intentions of the Council towards them. The information/data which is held, is held in manual and electronic record format and falls within the ambit of the DPA 1998, which since 1 March 2000 is the key legislation governing the protection and use of personal information.

Note that the DPA 1998 does not apply to deceased individuals.

The concept of data protection covers the standard to be applied when handling information about service users and the practices to be followed in order to achieve and maintain those standards. The guidelines to “*good practice*” are set out within the eight data protection principles as provided for within Schedule 1 of the DPA 1998. (Appendix B of the Information Sharing General Protocol details all the principles.)

The requirement to Share Information Fairly and Lawfully:

This first data protection principle is crucial when considering whether information can be shared.

Principle 1 requires that personal data shall be processed fairly and lawfully, and shall not be processed unless one condition in Schedule 2 is met and in the case of “*sensitive personal data*”, one condition in Schedule 3 must also be met.

“Processing” includes obtaining, recording, holding, organising, adapting, amending and **disclosing** information.

“*Sensitive personal data*” is defined in section 2 of the DPA 1998 and includes:

- data with respect to an individual’s racial or ethnic origin;
- his/her political opinions;
- his/her religious beliefs or other beliefs of a similar nature;
- his/her trade union membership;
- his/her physical or mental health or condition;

- his/her sexual life;
- details with respect to the commission or alleged commission of any offence; and
- any proceedings for any offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of any court in such proceedings.

Fair Processing

In order to meet the fair processing requirements, the Council and the NHS must ensure that a service user is not misled as to the purpose for which his/her information will be used. An individual service user should be told at the point of first contact the identity of the data controller (i.e the Council), his nominated representative (Alan Kirkwood is the Council's Data Protection Officer), the purposes for which information will be processed and the likely consequences of collecting such data.

Lawful Processing

With respect to processing information lawfully, the DPA 1998 does not provide any guidance on the meaning of the word "*lawful*". A specific act which is unlawful, is an act which is contrary to some law, or something which is done without lawful excuse. It follows that personal information which is unlawfully obtained may therefore be information which is obtained as a result of a breach of the common law duty of confidentiality, a disclosure which is in breach of the Human Rights Act 1998 or the obtaining of the information by way of breaching an enforceable contractual agreement. The list is not exhaustive.

Statutory grounds for disclosure

Disclosure without the consent of the service user can take place for a number of statutory purposes. The DPA 1998 therefore places no barrier to disclosure of such information. Typically, this will involve information relating to the investigation of crime or the detection and prosecution of offenders.

Where a child is considered to be at risk/child protection issues arise, the Council would have a statutory ground to disclose information in this respect and a section 29 exemption to the DPA 1998 would apply. [section 29(1)(a) the prevention or detection of crime (i.e. against that child). Section 29 exempts personal data from the subject information provisions¹ of the DPA 1998 and the non-disclosure provisions² of the DPA 1998.]

Thus a disclosure could be made where a child protection matter is prevalent.

¹ The first data protection principle to the extent to which it requires compliance with paragraph 2 of Part II of Schedule I (fair processing requirement)and section 7 (subject access).

² The first data protection principle except to the extent to which it requires compliance with Schedule 2 and 3 Conditions, the second, third and fourth data protection principles and section 10(a data subject's right to prevent processing likely to cause damage or distress) and 14(1) to (3) (rectification, blocking , erasure and destruction of data).

However, where a statutory ground for disclosure exists then consideration still needs to be given to Schedule 2, and in the case of sensitive personal information, Schedule 3 conditions and these will still require to be met before a disclosure is made in these circumstances although the fair processing code will not require to be satisfied (i.e. in particular the data subject will not require to be told about the disclosure) if the section 29 exemption is being relied upon.

Schedule 2 and Schedule 3 conditions

The relevant conditions are listed in **Appendix a**. Remember that personal data shall not be disclosed unless one condition in Schedule 2 is met and in the case of “*sensitive personal data*”, one condition in Schedule 3 must also be met.

The Schedule 2 and 3 conditions which may be relied upon where child protection matters are at issue are:-

- a) If the child’s life is at stake:-

Schedule 2, Para. 4
Schedule 3, Para. 3 (a)

- b) Where there is risk that a child may be the subject of an unlawful act or the prevention of an unlawful act against the child:

Schedule 2, Para. 5 (d)
Schedule 3, Para. 10 (SI 2000/417 refers³)

- c) General Child Protection matters (see “Sharing of Information About Children at Risk: A Guide to Good Practice” – Scottish Executive Publication 2003):-

Schedule 2, Para. 5 (b)
Schedule 3, Para. 7 (b)

Legal advice should be sought where there is any doubt.

³ SI 2000/417 meets condition 10 of Schedule 3 – it allows for the processing of personal data where it is in the substantial public interest; is necessary for the prevention or detection of **any unlawful act**; and must necessarily be carried **out without the explicit consent of the data subject being sought so as not to prejudice those circumstances**.

This section is relevant to Part C of the Form

This section contains general information on the requirements of the Human Rights Act 1998, lists the questions that need to be considered and then provides answers to the questions.

Human Rights Act 1998 – (HRA 1998)

The European Convention on Human Rights (ECHR) has been given direct legal effect in the UK by the HRA Act 1998. This Act came into force in the UK on 2 October 2000. In terms of Section 6 of that Act, public authorities, including the Council, may not act in a manner incompatible with Human Rights. If a public authority is found to have acted in breach of this provision, the authority is acting unlawfully and liable to pay the victim compensation.

Actions must therefore be in line with this Act.

Article 8.1 of the ECHR, provides that

“everyone has the right to respect for his private and family life, his home and his correspondence.”

Article 8 should therefore be given due consideration before any action is taken by which may infringe an individual’s rights in this respect.

Article 8 is however a qualified right, i.e. there are specified grounds upon which it may be legitimate to infringe or limit those rights.

Article 8.2 provides

*“there shall be no interference by a public authority with the exercise of this right **except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others**”.*

If there is no consent obtained from a service user with respect to the sharing of his/her information, a service user’s Article 8 rights would require to be considered before a disclosure could be made.

In assessing whether there has been a violation of this right and whether or not this is justified, the relevant issues are as follows:-

1. Is there an interference with the right in question?
2. Is the interference in accordance with the Law?
3. Does the interference have a legitimate aim or aims?
4. Is the interference necessary in a democratic society?
5. Is the interference discriminatory?

Taking each of these in turn:

1. Is there an interference with Article 8 if personal data is disclosed?

Disclosing personal data and sensitive personal data without the consent of the service user would be regarded as an interference with the rights prescribed in terms of Article 8.

2. Is interference in accordance with the Law?

There are two aspects to this. The interference must be lawful under Domestic Law and also meet the European Convention Test of Legality.

a. Domestic Law

The Council is a data controller in terms of the Data Protection Act (DPA)1998.

Disclosure of personal information stored in computer and manual records must be in accordance with the Act for there to be a lawful interference with the convention right.

Reference should be made to the previous section in this Guidance in order to determine if disclosure of information would be in accordance with this Act. If it would be, then an interference would be in accordance with domestic law.

A disclosure would also have an implied legal basis enshrined in statute ie the Children (Scotland) Act 1995 which embraces the concept of child protection matters. Where crimes are committed against children Schedule 1 of the Criminal Procedure (Scotland) Act 1995 would also be a pertinent legal basis upon which to rely.

b. Convention test of Legality

The domestic law in question must itself meet certain requirements, notably of accessibility and foreseeability. These are aspects of the objective of legal certainty.

Thus there must be a measure of legal protection against arbitrary interference by public authorities with the rights safeguarded. There must also be a degree of foreseeability, so as to allow a person to adapt his conduct. In short, the law must make clear the circumstances in which and the conditions under which the authority is empowered to interfere with the prescribed rights.

The domestic acts mentioned above meet these requirements.

3. Does the interference have a legitimate aim or aims?

The possible legitimate aims are set out in Article 8.2⁴ above. As regards the disclosure of information, the legitimate aim(s) pursued could be, typically, one or more of the following:

- the protection of health/morals;
- the prevention of crime;
- the protection of the child's rights and freedoms.

4. Would the interference be necessary in a democratic society?

This suggests some pressing social need and requires the reasons for any interference i.e. disclosure, to be both relevant and sufficient. It also involves a test of proportionality which involves weighing the balance on the individual's right to respect for their privacy against other statutory responsibilities. In other words, the disclosure of information must be proportionate to the aim being pursued. The aim pursued should be achieved in a minimalistic way.

Depending upon the circumstances of the individual case there may be a "*pressing social need*" to make a disclosure in the interests of child protection which cannot be effected in a minimal way.

⁴ In accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

5. Is the interference discriminatory?

Article 14 of the ECHR prohibits differential treatment of service users when considering their convention rights, in our case Article 8. In other words, all service users must be treated equally when reaching a decision regarding interference with their Article 8 rights. Therefore decisions taken to disclose information should be in line with decisions taken for other service users in similar situations.

Legal advice should always be sought where there is any doubt.

This section is relevant to Part D of the Form

This section contains general information on the common law duty of confidentiality and suggests some public interest justifications for disclosure in certain situations.

The Common Law Duty of Confidentiality

Scots law recognises a general obligation not to disclose information given in confidence. There is no limit on the type of information that is protected, it is the fact that it is given in confidence which is important.

For the purposes of the common law duty of confidentiality, the duty of confidence only applies to identifiable information that can be linked to a specific individual. Where personal information cannot be linked to an individual, then the common law concept of confidentiality will not apply.

Unless there is a statutory requirement to use the information which has been provided in confidence, then the information should only be used for the purposes for which an individual has been informed, and to which an individual has given his/her consent.

However, the common law duty of confidentiality is not absolute, and can be overridden by the holder of the information, where it can be justified that the disclosure of such information is within the public interest, for example to protect others from harm; for the prevention or detection of crime etc.

Unless there is a sufficiently robust public interest justification for disclosing identifiable information that has been provided in confidence, then the consent of the service user should always be sought. Where no consent is gained or forthcoming, then the need for confidentiality would require to be balanced against countervailing public interests¹.

Where child protection is the issue and a disclosure of personal data is required, the member of staff will require to justify under the common law duty of confidentiality, why it is considered necessary to disclose the specific information. This will be dependent upon the circumstances of each individual case.

Where a member of staff has evidence that a child may be at risk and/or child protection matters are at issue, then the countervailing public interest which would determine disclosure, would be the requirement to protect the child from harm; the prevention or detection of crime; a pressing social need.

Note that this duty of confidentiality still applies to information relating to deceased individuals

Legal advice should be sought where there is any doubt.

¹ Per Lord Goff in *Coco v A N Clark (Engineers) Ltd.*, [1969] RPC 41 at pp 48:- “Although the basis of the law on the protection of confidence is that there is a public interest that confidence should be preserved and protected by the law, nevertheless that public interest may be outweighed by some countervailing public interest which favours disclosure. This limitation may apply to all kinds of confidential information. It is this limiting principle which may require a court to carry out a balancing operation weighing the public interest in maintaining a confidence against a countervailing public interest in favouring disclosure.”

DATA PROTECTION ACT 1998

SCHEDULE 2: CONDITIONS RELEVANT FOR THE PROCESSING OF ANY PERSONAL DATA

Sharing information is necessary:-

- for the performance of a contract to which the service user is a party, or for the taking of steps, at the request of the service user, with a view to entering into a contract. [Para. 2].
- for compliance with any legal obligation to which the Council is subject, other than an obligation imposed by contract. [Para. 3].
- to protect the vital interests of the service user. [Para. 4].
- for the administration of justice. [Para. 5(a)].
- for the exercise of any functions conferred on any person by or under any enactment [Para. 5(b)].
- for the exercise of any functions of the Crown, a Minister of the Crown or a government department [Para. 5(c)].
- for the exercise of any other functions of a public nature exercised in the public interest [Para. 5(d)].
- for the purpose of legitimate interests pursued by the Council or by a third party or parties to whom the information is disclosed, except where the sharing of information is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the service user [Para. 6].

DATA PROTECTION ACT 1998

SCHEDULE 3: CONDITIONS RELEVANT FOR THE PROCESSING OF SENSITIVE PERSONAL DATA

Sharing information is necessary:-

- for the purposes of exercising or performing any right or obligation, which is conferred or imposed by law on the Council in connection with employment [Para. 2].
- in order to protect the vital interests of the service user or another person, in a case where –

consent cannot be given by or on behalf of the service user, or the Council cannot reasonably be expected to obtain the consent of the service user [Para. 3(a)], or

in order to protect the vital interests of another person, in a case where consent by or on behalf of the service user has been unreasonably withheld [Para. 3(b)].
- [Para. 4]
 - a) is carried out in course of its legitimate activities by any body or association which - is not established or conducted for profit, and exists for political, philosophical, religious or trade-union purposes,
 - b) is carried out with appropriate safeguards for the rights and freedoms of service users,
 - c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
 - d) does not involve disclosure of the information to a third party without the consent of the data subject.
- The information has been made public as a result of steps deliberately taken by the service user [Para. 5].
- For the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) [Para. 6(a)].
- For the purpose of obtaining legal advice [Para. 6(b)].
- Otherwise for the purposes of establishing, exercising or defending legal rights [Para. 6(c)].
- For the administration of justice [Para. 7(a)].
- For the exercise of any functions conferred on any person by or under an enactment [Para. 7(b)].

- For the exercise of any functions of the Crown, a Minister of the Crown or a government department [Para. 7(c)].
- For medical purposes and is undertaken by [Para. 8] -
 - a) a health professional, or
 - b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

In this paragraph “medical purposes” includes the purposes of preventative medicine, medical research, the provision of care and treatment and the management of healthcare services.

- [Para. 9] -
 - a) is of sensitive personal data consisting of information as to racial or ethnic origin,
 - b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
 - c) is carried out with appropriate safeguards for the rights and freedoms of service users.

- [Para. 10] –

The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

To date the only order made under this paragraph is the Statutory Instrument 200/417 **Data Protection Act (Processing of Sensitive Personal Data) Order 2000**. This Order specifies other circumstances in which sensitive personal data may legitimately be processed. These are:-

1. – (1) The processing –
 - (a) is in the substantial public interest;
 - (b) is necessary for the purposes of the prevention or detection of any unlawful act; and
 - (c) must necessary be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.
- (2) In this paragraph, “act” includes a failure to act.
2. The processing –
 - (a) is in the substantial public interest;
 - (b) is necessary for the discharge of any function which is designed for protecting members of the public against-

- (i) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person, or
 - (ii) mismanagement in the administration of, or failures in services provided by, any body or association; and
- (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the discharge of that function.

3. -(1) The disclosure of personal data –

- (a) is in the substantial public interest;
 - (b) is in connection with –
 - (i) the commission by any person of any unlawful act (whether alleged or established),
 - (ii) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person (whether alleged or established), or
 - (iii) mismanagement in the administration of, or failures in services provided by, any body or association (whether alleged or established);
 - (c) is for the special purposes as defined in section 3 of the Act; and
 - (d) is made with a view to the publication of those data by any person and the data controller reasonably believes that such publication would be in the public interest.
- (2) In this paragraph, “act” includes a failure to act.

4. The processing –

- (a) is in the substantial public interest;
- (b) is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service; and
- (c) is carried out without the explicit consent of the data subject because the processing –
 - (i) is necessary in a case where consent cannot be given by the data subject,
 - (ii) is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject, or
 - (iii) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, advice, support or other service.

5. – (1) The processing –

- (a) is necessary for the purpose of –
 - (i) carrying on insurance business, or
 - (ii) making determinations in connection with eligibility for, and benefits payable under, an occupational pension scheme as defined in section 1 of the Pension Schemes Act 1993.
- (b) is of sensitive personal data consisting of information falling within section 2(e) of the Act relating to a data subject who is the parent, grandparent, great grandparent or sibling of –
 - (i) in the case of paragraph (a)(i), the insured person, or
 - (ii) in the case of paragraph (a)(ii), the member of the scheme;

- (c) is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of that data subject and the data controller is not aware of the data subject withholding his consent; and
- (d) does not support measures or decisions with respect to that data subject.

(2) In this paragraph –

- (a) “insurance business” means insurance business, as defined in section 95 of the Insurance Companies Act 1982, falling within Classes I, III or IV of Schedule 1 (classes of long term business) or Classes 1 or 2 of Schedule 2 (classes of general business) to that Act, and
- (b) “insured” and “member” includes an individual who is seeking to become an insured person or member of the scheme respectively.

6. The processing -

- (a) is of sensitive personal data in relation to any particular data subject that are subject to processing which was already under way immediately before the coming into force of this Order;
- (b) is necessary for the purpose of –
 - (i) carrying on insurance business, as defined in section 95 of the Insurance Companies Act 1982, falling within Classes I, III or IV of Schedule 1 to that Act; or
 - (ii) establishing or administering an occupational pension scheme as defined in section 1 of the Pension Schemes Act 1993; and
- (c) either –
 - (i) is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject and that data subject has not informed the data controller that he does not so consent, or
 - (ii) must necessarily be carried out even without the explicit consent of the data subject so as not to prejudice those purposes.

7. (1) Subject to the provisions of sub-paragraph (2), the processing -

- (a) is of sensitive personal data consisting of information falling within section 2(c) or (e) of the Act;
- (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons –
 - (i) holding different beliefs as described in section 2(c) of the Act, or
 - (ii) of different states of physical or mental health or different physical or mental conditions as described in section 2(e) of the Act;with a view to enabling such equality to be promoted or maintained;
- (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and
- (d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

(2) Where any individual has given notice in writing to any data controller who is processing personal data under the provisions of sub-paragraph (1) requiring that data controller to cease processing personal data in respect of which that individual is the data subject at the end of such period as is reasonable in the circumstances, that data controller must have ceased processing those personal data at the end of that period.

8. – (1) Subject to the provisions of sub-paragraph (2), the processing –

- (a) is of sensitive personal data consisting of information falling within section 2(b) of the Act;
- (b) is carried out by any person or organisation included in the register maintained pursuant to section 1 of the Registration of Political Parties Act 1998 in the course of his or its legitimate political activities; and
- (c) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

(2) Where any individual has given notice in writing to any data controller who is processing personal data under the provisions of sub-paragraph (1) requiring that data controller to cease processing personal data in respect of which that individual is the data subject at the end of such period as is reasonable in the circumstances, that data controller must have ceased processing those personal data at the end of that period.

9. The processing –

- (a) is in the substantial public interest;
- (b) is necessary for research purposes (which expression shall have the same meaning as in section 33 of the Act);
- (c) does not support measures or decisions with respect to any particular data subject otherwise than within the explicit consent of that data subject; and
- (d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

10. The processing is necessary for the exercise of any functions conferred on a constable by any rule of law.