GUIDANCE ON DEALING WITH DISCLOSURE OF INFORMATION TO THIRD PARTIES – GENERALLY

Contents **Page No**

Introduction

This note provides guidance in relation to access to Service User's Case Files by Social Work Service Representatives. It also covers the disclosure of any personal information about Service Users to third parties generally, whether they are Council employees working in other departments, or from outside the Council entirely.

It is possible, and on occasions essential, for information about Service Users to be disclosed by staff. Disclosing information held about Service Users 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 document contains guidance for staff in dealing with this sensitive issue and is the guidance referred to in Section 9(b) of the Case Recording Policy.

No matter the form of disclosure, Social Work Service Representatives should ensure that they are in compliance with the Case Recording Policy and this Guidance, in making such disclosure.

Note that there is separate Guidance on Disclosing Information to Third Parties in Order to Protect a Child Considered to be at Risk.

Disclosure to Council Employees

Personal information in relation to a Service User is available to Social Work Representatives working with the Service User.

It is recognised that information given to an individual social worker for a specific purpose may require to be disclosed to other Social Work Service Representatives where the management of the case requires it. Any such disclosure should take place in accordance with established policy and procedures.

Social Work Service Representatives may require to consult a Case File or Case Record of a Service User to whom they are not involved in providing services. They may do so, provided that it is demonstrated to the relevant line managers that the information is required to facilitate the care or welfare of any Service User to whom any such Social Work Service Representative is involved in providing services.

A limited range of other Council employees may require access to Service Users' personal information in order to carry out their duties in or in connection with the provision of services to the Service User.

These include:

- **Legal Advisers**
  When actual or possible court proceedings arise, or when legal advice is otherwise required.

- **Other departments**
  Of the Council for the purposes of obtaining services for the Service User.

- **Researchers**
  Engaged in evaluative studies and other investigations relating to service provision by the Social Work Service.
  (See later for more guidance on this.)

Disclosure to Third Parties With Consent

Party to a General Protocol for the Sharing of Information

Information Sharing Protocols have been developed that have been designed to ensure that the exchange of information, which is necessary to permit multi-organisational and multi-disciplinary service provision, can proceed in a way which conforms with all applicable laws and safeguards the rights of Services Users.

Where the Council has signed up to a General Protocol (and currently it has for Adult Services and will shortly for Children & Young People's Services) 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.

The purposes for sharing information, listed in both General Protocols (for Adult services and for Children & Young People's Services), are:

- To support national initiatives on multi-organisational working and information exchange;
- To provide professionals with the information which they will require to deliver integrated services;
- To improve the quality of services for Service Users in Grampian;
- To produce consistent services and information;
- To enhance the robustness and effectiveness of systems to protect Service Users from harm;
- To support a single point of access and out of hours service to the Grampian children and young people;
- To support joint care planning and commissioning;
- To support statutory reporting functions and effective use of resources;
- To assist the management teams of the partnership organisations with planning and the management of information;
- To enable the partnership organisations to review, account for and improve the services which they provide to Service Users;
- To achieve more desirable outcomes for individuals receiving care.

Additional purposes for sharing information, listed in the General Protocol for Children & Young People's Services only, are:

- To meet the needs and duties of the partnership organisations;

- To reduce duplication;
- To protect children and young people.

Therefore, if consent is in place, there are no barriers to sharing information for these purposes, when necessary, with the other organisations who have signed the Protocol.

Other Third Parties

In the course of the provision of its services to Service Users, the Social Work Service may be asked to pass information to other individuals, agencies or organisations, in order to facilitate service provision. For example:

- Welfare/Benefit agencies.
- Probation Service and Local Authority Social Services outside Scotland.
- Other Local Authority Social Work Services.

Personal information about a Service User should only be given to any such parties in accordance with the principles set down in the Case Recording Policy and after obtaining the explicit consent of the Service User.

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.

Personal information must be disclosed only on a need to know basis, therefore only that which is required by the party seeking disclosure in order to provide a service to the Service User must be disclosed. Where a member of staff has concluded that disclosure is necessary for this purpose then that member of staff should ensure that an audit trail is kept on file to support this conclusion 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.

Disclosure to Third Parties 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.

Miscellaneous

Disclosure through the Media

The decision to disclose personal information and make this publicly available or by advertisement may be made by the Designated Manager after completion of the Decision to Share Information Without Consent Form. However, any personal information made available through the media should be restricted to that which is entirely necessary.

Any press release should therefore be forwarded to the Head of Legal Services prior to publication, having first been approved by the appropriate Head of Service. The completed Form should be forwarded to Legal services at the same time.

Councillors and MSPs/MPs

Councillors and MSPs/MPs have no particular rights of access to information about others unless Service User permission has been given. They may however act as an agent, provided that it can be established that they are acting as an authorised agent of the Service User. See the Guidance on Dealing With Subject Access Requests Under the Data Protection Act 1998.

Education

Students in training must work in collaboration with a Social Work Service employee who will take responsibility for ensuring that this Case Recording Policy is understood and followed. Any personal data contained in a Case File which is used for teaching or education purposed should be anonymised (so that the subject of the data cannot be identified) in accordance with departmental policy.

Research

The provision of information about individual Service Users to research workers requires the prior approval of the appropriate Head of Service. Research workers must be asked to provide formal undertakings that they, and their research team, will:

- Comply with Social Work Service policies and procedures, including this Case Recording Policy and the Social Work Service's Case Recording Procedures document;

- Not approach the subject or donor of any personal information provided to them by the Social Work Service;

- Not disclose personal information outside their research team;

- Ensure that no individual Service User is identifiable from published material;

- Adequately secure any personal information provided to them by the Social Work Service against unauthorised access, damage or destruction; and

- Destroy all personal information obtained from the Social Work Service for the purpose of the research, within a specified period.

Reports and Records in Court Proceedings

Neither the Procurator Fiscal, representatives of Crown Office nor any independent solicitor can demand that Social Work Service records are released, or details from those records be disclosed, unless an appropriate court order has been obtained.

The Procurator Fiscal must apply to the Sheriff Court or to the High Court of Justiciary for a warrant to obtain any documents required for prosecution, including Social Work Service records. Similarly, criminal defence solicitors must apply to the particular Court for an order before they are entitled to recover documents, which may assist in the defence of a criminal case.

Solicitors on both sides in civil actions must apply to the Sheriff Court or the Court of Session for an order to release any Social Work Service records to them.

Once such orders are obtained, whether in civil or criminal cases, they require to be served formally on The Moray Council.

In criminal proceedings, it is the function of the Sheriff Clerk if the case is being prosecuted in the Sheriff Court, or the Clerk of Justiciary in the High Court, to make reports available to other parties. All requests to see reports should be directed to the relevant Clerk.

The Social Work Service may claim that certain documents are confidential and the court then has to decide whether or not the documents are to be released. There are grounds for pleading confidentiality for any reports or records **not** prepared for the particular case in question but, in all cases, advice should be sought from Legal Services before showing, discussing or releasing any documents. Other grounds to support the withholding of documentation may exist in certain cases.

The Procurator Fiscal may cite Social Work Service Representatives as witnesses to provide support for the prosecution of an offence. Similarly, a criminal defence solicitor is entitled to cite Social Work Service Representatives as witnesses for the defence of a criminal case. Social Work Service Representatives are obliged to appear as witnesses when cited. If contacted by either side's representatives in a court case in relation to Social Work records, advice should be sought from Legal Services before speaking with the representatives.

Appendix 1

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)

Appendix 2

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 disclosing information to the Police for the investigation of crime or the detection and prosecution of offenders. [Section 29(1)(a) the prevention or detection of crime. Section 29 exempts personal data from the subject access provisions[1] of the DPA 1998 and the non-disclosure provisions[2] of the DPA 1998.]

Should there be any doubt in any case that a statutory ground to disclose applies, Legal Services must be contacted to confirm this.

[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).

The police will have the option of seeking a court order if local authorities, or individual social workers, decline to disclose personal information. In these circumstances the Social Work Service would then have a legal obligation to disclose the personal information requested by the police, as described below (see paragraph headed "Requirement by a Court").

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 as 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 DPA 1998 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.

In relation to Schedule 2, para.3, the Social Work Service can be legally obliged to disclose personal information by an enactment (Act of Parliament/statute), rule of law or order of a court.

By way of example only, a legal obligation to disclose personal data *may* be owed to any of the following individuals in terms of an enactment: Commissioner for Local Administration; Officers of the Secretary of State; Members of a Committee of Enquiry; Mental Welfare Commission; Responsible Medical Officer; Council and Scottish Office Auditors; Central Government Social Work Services (for statutory and statistical purposes).

A legal obligation may also arise in the following circumstances:

<u>Requirements by a Court</u>

The courts have power to order the production of existing documents e.g. Case Records and Case Files. In such circumstances the advice of Legal Services should be sought.

The courts can also instruct the writing of a report for a specific case. Reports must be given directly to the Sheriff Clerk. Any enquiries from other parties involved in the case should be directed to him.

<u>Requirements by Children's Hearing</u>

The Reporter may require the Social Work Service to provide Social Work Reports for the Children's Panel.

Disclosure of Safeguarders, Curators ad Litem and Reporting Officers

Children's Hearings may appoint persons to safeguard the interests of the child in proceedings where there is or may be, a conflict of interest between people with parental rights and responsibilities, and the child. Any such safeguarder is entitled to receive any papers that are made available to the Hearing members, including the Social Background Report.

Curators ad Litem may also be appointed in the interests of safeguarding children and vulnerable adults in court proceedings. Any such Curator ad Litem is entitled to receive any papers, which are made available, including the Social Background Report to enable them to carry out their duties.

The Social Work Service may consider it necessary for personal information to be disclosed in order to prevent danger or serious risk to public health. Medical advice should be sought as to the necessity and manner of disclosure.

Sharing information without consent where the service user is incapable of providing consent and the provision of services is necessary for the health and well being of the service user.

In a case where the relevant professional in exercise of his or her best professional judgement, entertains reasonable doubts as to the capacity of a service user (which includes a potential service user) to give consent to the processing of service user personal data, the individual's capacity to give consent requires to be assessed in accordance with the Adults with Incapacity (Scotland) Act 2000 and following the procedure for assessment set out in the *Information Sharing: Practitioner Guidance***.**

Where the relevant professional,

- following the assessment procedure, determines that a service user is incapable of giving consent,
- determines that no other person has been legally appointed to consent on the service user's behalf and it is not intended that someone be appointed,
- has considered the further factors detailed in the Information Sharing General Protocol,
- has decided that provision of services is necessary for the health and well being of the service user,
- has completed Part A of the Form with all relevant information,

then service user personal data may be shared to the extent necessary to provide services, notwithstanding the lack of consent by the service user.

Schedule 2, para 5(b) would apply in this instance, as would Schedule 3, para. 7(b).

This would cover

- **sharing necessary information contained in the Single Shared Assessment to enable a Care Plan to be developed;**

- **the sharing of Care Plans to ensure consistent care;**

- **The sharing of information regarding a service user's well being, activity, needs etc. on a daily basis to ensure that appropriate support is provided; and**

- **case discussions at weekly team meetings.**

This would also apply where a service user does have capacity but for whatever reason, has not provided consent to disclosure, but only to the extent absolutely necessary to provide essential services.

Sharing information without consent where the service user is incapable of providing consent and the service user is at risk.

Where a service user is considered to be vulnerable and at risk e.g. from sexual assault or other abuse, fraud etc., there would be 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 a crime (i.e. against that service user).

The Schedule 2 and 3 conditions which may be relied upon are:-

a) If the Service User's life is at stake:-

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

b) Where there is risk that a Service User who lacks capacity may be the subject of an unlawful act or the prevention of an unlawful act against the Service User:

Schedule 2, para. 5 (d)
Schedule 3, para. 10 (SI 2000/417 refers[3])

This would also apply where a Service User does have capacity but for whatever reason, has not provided consent for disclosure.

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.

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

forseeability, 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 DPA 1998 mentioned above meets these requirements.

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

The possible legitimate aims are set out in Article 8.2[4] 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 minimilistic way.

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.

[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".

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 interests[1].

Where 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 Service User's safety or health and wellbeing may be at risk, then the countervailing public interest which would determine disclosure, would be the requirement to protect the Service User from harm and the need to ensure the adult's safety, health and wellbeing.

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."

Appendix a

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 thatn 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.