Appendix B to PIPOT Protocol:
Best Practice guidance when deciding to disclose information:

1. The default position should be that the owner of the information (data owner) about a person in a position of trust should not share it without the person's knowledge and permission, unless doing so would increase risk to the adult(s) involved or others. The person in a position of trust should be encouraged to share the information with their own employer(s) first. If they decline to share it with their employer(s) for whatever reason, this does not mean the information cannot be shared. In deciding whether to nevertheless share the information with an employer, student body or voluntary organisation, the following principles should be followed:

2. If the person in a position of trust asks the data owner not to share the information, a decision must be made in line with the principles contained within this guidance.

3. If it is agreed that information will not be shared, this must be qualified since it may be the case that more detail comes to light to change this decision. If a decision is made at a later date to share information, the person in a position of trust should be consulted again and given a further opportunity to disclose the information him or herself if it is appropriate to do so. Again, the data owner could decide to share the information even if the person in a position of trust decides not to. All decisions to share or not share information, and their rationale should be clearly recorded.

4. In each case involving an allegation or concern against a person in a position of trust, a balance has to be struck between the duty to protect people with care and support needs from harm or abuse and the effect upon individuals of information about them being shared, for example, upon the person's Human Rights (Article 8- the right to private and family life).

5. For these reasons each case must be considered on its own merits and personal data shall be processed in accordance with the principles contained in Part I of Schedule 1 of the Data Protection Act 1998 ("the DPA"):

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

6. Due regard must be had to Article 8 of the European Convention on Human Rights, which states that:

Everyone has the right to respect for his private and family life, his home and his correspondence.

And

There shall be no interference by a public authority with the exercise of this right except such 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.

7. When deciding whether to interfere with a person's Article 8 rights, each case must be judged on its own facts. The issue is essentially one of proportionality. Information is to be disclosed only if there is a "pressing need" for that disclosure. In considering proportionality, consideration should be given to the following general principles:

- The legitimate aim in question must be sufficiently important to justify the interference.
- The measures taken to achieve the legitimate aim must be rationally connected to it.
- The means used to impair the right must be no more than is necessary to accomplish the objective.
- A fair balance must be struck between the rights of the individual and the interests of the community; this requires a careful assessment of the severity and consequences of the

interference.

"There is a general presumption [which is not absolute] that information should not be disclosed, such a presumption being based upon a recognition of (a) the potentially serious effect on the ability of [in this case convicted people] to live a normal life; (b) the risk of violence to such people and (c) the risk that disclosure might drive them underground."

8. Before disclosing information to a third party, there is a need to consult with the person whose information is to be disclosed and to give them an opportunity of making representations before the information is disclosed.

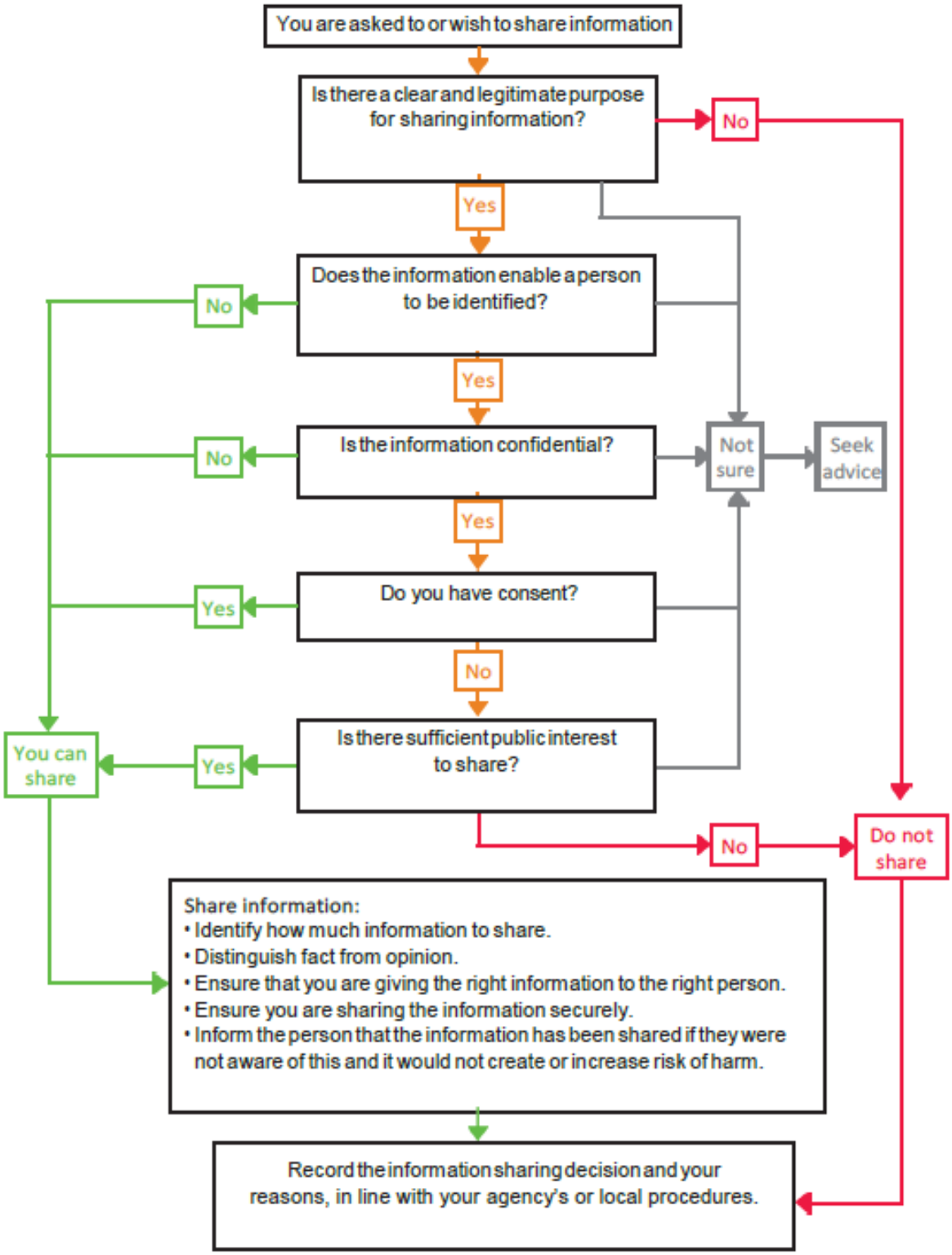
"[T]he imposition of such a duty is a necessary ingredient of the process if it is to be fair and proportionate."

9. Information may be shared by an individual or an agency in the expectation that it will not be shared with others; i.e. it will be kept confidential. Confidential information can be shared if it is justified as being in the public interest (e.g. for the detection and prevention of crime and for the protection of vulnerable persons, i.e. children or adults with care and support need). It is a matter for professional judgment, acting in accordance with information sharing protocols and the principles of the DPA to decide whether breaching the person in a position of trust's confidentiality is in the public's interest.

10. If after following the above principles, and weighing up the information available, a decision is made not to tell the person in a position of trust about the concern about them and ask their permission to share it with their employer, because doing this would place any adults or children at increased risk of harm, then this decision and the reasons for it should be recorded. However, further planning processes must identify the earliest opportunity for them to be informed.

10 Disclosures to employers should be made without unnecessary delay. If the disclosure is made verbally to the employer, it is best practice to follow this up in writing to outline exactly what information has been shared. A copy of this can be shared with the person in a position of trust if this is appropriate, and if this will not increase risk.

Flowchart of key questions for information sharing



If there are concerns that a child may be at risk of significant harm or an adult may be at risk of serious harm, then follow the relevant procedures without delay.

Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.

Further information about relevant legislation – this does not substitute for legal advice where required.

Both the Data Protection Act 1998 and GDPR regulate the use of "personal data". To understand what personal data means, we need to first look at how the Act defines the word "data".

"data" means information which—
(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68; or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)

What is personal data?

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

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and involves any expression of opinion about the individual and any indication of the intentions of the Data Controller, or any other person in respect of the individual.

Sensitive personal data, also known as special category data, in Article 9 of the GDPR means personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- his/her political opinions,
- his/her religious beliefs or other beliefs of a similar nature,
- whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his/her physical or mental health condition,
- his/her sexual orientation,
- the commission or alleged commission by him/her of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

The Act regulates the "processing" of personal data. Processing in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available,
- alignment, combination, blocking, erasure or destruction of the information or data,

Data Protection Principles:

Schedule 1 to the Data Protection Act 1998 and Article 5 of the GDPR lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless :

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this act.

7. Appropriate technical and organisational measures shall be taken again unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

Section 1(4) of the Data Protection Act says that:

"Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act, the data controller."

This means that where an organisation is required by law to process personal data, it must retain data controller responsibility for the processing. It cannot negate its responsibility by 'handing over' responsibility for the processing to another data controller or data processor. Although it could use either type of organisation to carry out certain aspects of the processing for it, overall responsibility remains with the organisation with the statutory responsibility to carry out the processing.

To determine whether you are a data controller you need to ascertain which organisation decides:

- to collect the personal data in the first place and the legal basis for doing so,
- which items of personal data to collect, i.e. the content of the data,
- the purpose or purposes the data are to be used for,
- which individuals to collect data about,
- whether to disclose the data, and if so, who to,
- whether subject access and other individuals' rights apply i.e. the application of exemptions; and
- how long to retain the data or whether to make non-routine amendments to the data.

These are all decisions that can only be taken by the data controller as part of its overall control of the data processing operation.

Data Protection Act 1998:

SCHEDULE 2: Conditions relevant for purposes of the first principle: processing of any personal data

1 The data subject has given his consent to the processing.

2 The processing is necessary—

(a) for the performance of a contract to which the data subject is a party, or

(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3 The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4 The processing is necessary in order to protect the vital interests of the data subject.

5 The processing is necessary—

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under any enactment,

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

SCHEDULE 3 Conditions relevant for purposes of the first principle: processing of sensitive personal data

1 The data subject has given his explicit consent to the processing of the personal data.

2(1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order—

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3 The processing is necessary—

(a) in order to protect the vital interests of the data subject or another person, in a case where—

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4 The processing—

(a) is carried out in the course of its legitimate activities by any body or association which—

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(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 personal data to a third party without the consent of the data subject.

5The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6 The processing—

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

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

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

7(1) The processing is necessary—

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order—

(a)exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8(1) The processing is necessary for medical purposes and is undertaken by—

(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.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9(1) The processing—

(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 data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

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