Excerpted from: https://www.farrer.co.uk/globalassets/clients-and-sectors/safeguarding/low-level-concerns-guidance-2020.pdf

Appendix D

Low level-concerns and data protection

1. The overlap between safeguarding duties and data protection in general terms – duties of record keeping, retention and information sharing – is increasingly well-understood by practitioners. It is addressed by the Data Protection Act 2018 (**DPA 2018**), by statutory and non-statutory guidance provisions within KCSIE, and by DfE guidance on Information Sharing.

2. Although we currently have little in the way of specific DPA 2018 guidance from the Information Commissioner's Office (**ICO**) that is tailored to safeguarding practice, and/or the relevant sectors (for example, schools, charities, sports and religious organisations), the ICO's consultation draft **Information Sharing Code of Practice** (published 16 July 2019) does specifically cite safeguarding of children as a "clear example of a compelling reason" for personal data sharing, as well as recognising the role of regular multi-agency information sharing. The ICO has produced its guidance on the processing of special category data, which acknowledges safeguarding as part of its general guidance on "substantial public interest" conditions for processing, and provides a template for the appropriate policy document.[42]

3. Making records where substantive abuse or neglect is reasonably suspected can be comfortably aligned with the principles of data protection law. However, greater difficulties in (a) confirming the applicable lawful processing ground, and (b) balancing the safeguarding interest with personal data rights, are caused where the conduct in question does not in and of itself amount to an allegation but may, nonetheless, constitute concerning, problematic or inappropriate behaviour towards children, and even more so if it is potentially seen and evaluated as part of a pattern.[43]

4. The importance of sharing low-level concerns is explained in the main guidance, and the value to an organisation is dependent on such concerns being shared, recorded and retained over a period of time.

5. However, the issues that we are aware can arise in practice are:

   (a) staff not understanding possible indicators of organisational based grooming, and thus not sharing concerns about it (a training issue);

   (b) a reluctance by staff to share low-level concerns which, depending on the culture of an organisation, can be perceived as a heavy handed or even inappropriate approach;

   (c) uncertainty as to how and where information provided in the context of low-level concerns may lawfully be recorded and used, under what DPA 2018 ground, and how long it may be retained; and

   (d) which principles or exemptions apply to subject access requests to such (personal) data, and related data subject rights around transparency, erasure, and correction.

   As to (d), a common concern is that on-demand access by data subjects will be counter-productive to the intended objective and risks having a chilling effect on the rate of reporting/recording. We have considered reasons why this may not be so in the main guidance (at paragraph 7).

6. The legal and factual backgrounds (including the General Data Protection Regulation EU 2016/679 (**GDPR**)) have been considered in a longer paper by Hugh Davies QC and Owen O'Rorke, intended for consideration by government departments as the basis for potential guidance and, possibly, a case for some class exemption from subject access rules specific to this practice to be introduced in due course by way of statutory instrument. This Appendix addresses the situation as it currently stands (August 2019).

The intention and effect of the current law and guidance (in overview)

7. The DPA 2018 has made express provision, subject to certain conditions, for processing both Special Category Personal Data of a sensitive nature (SPD) and criminal records data where necessary for safeguarding purposes.[44] This provision (made by way of late amendment to the Data Protection Bill in March 2017) defines safeguarding widely as protecting a child (i.e. under the age of 18), or adult at risk, from neglect or physical, mental or emotional harm, or protecting their physical, mental or emotional well-being.[45]

8. In our view, the clear intention of Parliament in the cited DPA 2018 provisions was to clarify the lawful conditions under which safeguarding professionals

42 Information Commissioner's Office (2019) *Special Category Data*, accessed on 25 November 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/

43 A distinction is made in the main guidance between an allegation and a low-level concern, and a definition is given for each.

44 Paragraph 18 of Part 2 of Schedule 1 Data Protection Act 2018 (DPA 2018).

45 The safeguarding condition at paragraph 18 sits alongside other non-consent SPD and criminal data processing grounds in the DPA 2018 of relevance to safeguarding practitioners, whether new or amended from the DPA 1998. These include obligations imposed by law on employers; functions designed to protect the public from seriously improper conduct; standards of behaviour in sport; preventing or detecting unlawful acts; safeguarding the welfare of those at economic risk; providing support for individuals with a particular disability or medical condition by dedicated not-for-profits; and administration of accounts used in the commission of indecency offences involving children.

operate, and to remove any perceived barriers in data protection law for organisations in keeping children safe. This may be seen in both the new derogations from GDPR, and certain additions or amendments to the sector-specific provisions of the old Data Protection Act 1998 (**DPA 1998**).

9. However, the DPA 2018 has not released organisations or practitioners in this sector from the burdens imposed by GDPR in respect of data subject rights, transparency or accountability more generally. Indeed, the DPA 2018 has provided for some additional safeguards (such as the need for an "**appropriate policy document**" – see further, below) as part of the general requirement on organisations to map out and document the lawful basis for their personal data processing activities. This is all in line with the GDPR requirement that any such national derogations still respect the essence of the right to data protection.

10. The committee's experience is that many organisations, and many individual practitioners, are still uncertain as to how their responsibilities for safeguarding children sit with their obligations under data protection law. Although the DPA 2018 does substantially more to assist practitioners than the DPA 1998 did, the alarmist media coverage of GDPR has left many with the impression that the task of record-keeping and information sharing has got harder since 25 May 2018. This is true to some extent, in terms of administrative burden and the pro-active need to demonstrate compliance, but proving the underlying lawfulness of any processing necessary for safeguarding is now easier than before.

11. Two opposing schools of thought can often be observed among practitioners since GDPR:

(a) one is to believe that "because of GDPR", organisations should not collect, record or share certain information without consent; must delete records routinely; and are under a duty to amend or delete records when so requested by a data subject;

(b) the opposing view that, because child protection "trumps" data protection, safeguarding practitioners are exempt from or can safely disregard GDPR, and/or that safeguarding records are exempted from data subject rights.

12. Of these two, it is clear that (a) – a misguided excess of caution – carries the greater risk to children. However, to disapply data protection law altogether goes against the essence of individual privacy rights, erodes necessary checks and balances, and places organisations at regulatory risk. Additionally, better-prepared organisations who have audited their approach will be better placed to deal with subject access and erasure requests.

13. An area where we believe specific guidance and reassurance is required is in the approach to the recording of potentially valuable information about adults or children – whether by sharing low-level concerns or self-reporting – that does not meet the threshold of an allegation requiring referral to statutory agencies.

The tensions between low-level concerns policies and data protection law

14. Since the DPA 2018 there ought to be little or no tension between the application of data protection law to safeguarding information and the needs, or efficacy, of accepted safeguarding practice. When it comes to sharing and recording low-level, however, there are more nuanced and marginal balancing acts for data controller organisations to consider.

Legal basis for processing

15. In legal terms, not all the personal data that might be recorded as a low-level concern (e.g. small changes in behaviour, favouritism etc.) would necessarily constitute special category personal data (SPD) in isolation. However, it is prudent to consider that all information recorded to a safeguarding file, in a safeguarding context, should be treated as SPD.

16. The effect of GDPR is that, to process SPD, a data controller must satisfy both a condition under Article 6 GDPR and one under Article 9 GDPR. It is not the purpose of this guidance to consider every possible scenario applicable to practitioners, but it seems likely that for the former most data controllers will be relying on Article 6(1)(f) – namely, that processing is necessary in their (or another's) legitimate interests.

17. For the Article 9 condition, the DPA 2018 safeguarding provision works as follows. The necessity of "safeguarding of children and individuals at risk" (including from emotional, physical or sexual abuse and neglect) is a condition under which individuals or organisations are permitted to share, record or otherwise process SPD, even in circumstances where the person to whom such SPD relates has not explicitly (or otherwise) consented to the information being shared. That is provided that:

(a) to obtain explicit consent could not reasonably be expected of the controller, or is not possible, or might risk undermining the safeguarding purpose;

(b) the use of such personal data is necessary for such a safeguarding purpose in the substantial public interest; and

(c) the person or organisation relying on this ground can point to an "appropriate policy document" (see again below) setting out both how its needs meet the relevant condition, and explaining its policy on retention.

18. The EU and UK case law is clear[46] that in this context, both for 17 and 18(b), the word "necessary" does not require that a certain action is absolutely necessary, nor the only means to achieve a purpose. It is rather a case of what is reasonably necessary, applying EU principles of proportionality: that the use of the personal data clearly supports the purpose, is not excessive nor goes beyond what is reasonably required to fulfil the aim – in this case, the protection of children (or adults at risk).[47]

19. Whilst this does mean that controllers ought to use the least amount of personal data necessary to achieve the aim, it should not mean that controllers have to make any compromise in the efficiency of achieving the safeguarding purpose. When applied to low-level concerns policies: if the recording, sharing and retention of the personal data is reasonably held to be necessary in serving a safeguarding purpose, then it ought in our view to fall lawfully within the DPA 2018 condition.

20. There are the following caveats to this rule of thumb:

(a) there may be means for individuals whose personal data is recorded under the policy to object to the processing.[48]

(b) assuming that (in respect of the GDPR Article 9 condition required for the SPD) the data controller organisation is relying on the safeguarding condition under DPA 2018, it must first establish that explicit consent is not possible, or could reasonably be expected, for the controller to obtain without prejudicing the safeguarding purpose; and

(c) depending on the precise scope of the policy adopted by the organisation, the nature of the information held may be borderline in terms of the balance between value to the safeguarding purpose, and personal privacy intrusion – namely, the risk of "gossip" or prurience.

21. Provided that the safeguarding purpose is a valid one and those affected are fully notified of the policy, any difficulty in showing the legal basis can, in our view, be overcome by judicious means of a Data Protection Impact Assessment (**DPIA**) – a self-assessment tool – alongside relevant policies.

22. Beyond the legal basis, however, are the burdens placed on organisations by rules of accountability such as data subject rights and additional "appropriate policy documents".

The need for an Appropriate Policy Document

23. In order to rely on the DPA 2018 safeguarding provision cited above, an organisation must have an "appropriate policy document", demonstrating that it understands how the legal basis applies to it, and setting out their rationale and period for retention. It will need to be in place when the processing is carried out (and for at least 6 months thereafter); reviewed at suitable intervals; and made available on request to the ICO.

24. As part of its November 2019 guidance on the processing of special category data, the ICO has developed an appropriate policy document template, although it highlights that using this exact form is not a requirement.[49] An organisation may choose to have a stand-alone policy, such as the ICO template; or it may prefer to document its use of the safeguarding data processing condition within its existing policies around safeguarding, retention and/or data protection (including any low-level concerns policy). The important point is that these policies are all internally consistent, and refer to each other where relevant.

Retention of safeguarding files

25. A key element of such a policy would be **retention**. In the case of *R (C) v Northumberland County Council [2015] EWHC 2134 (Admin)*, the court:

(a) firmly upheld the data controller council's policy to keep safeguarding records for long periods – not simply to defend historic claims (for which limitation periods may be set aside) or allow the children concerned access in later life, but moreover for the purpose of protecting children;

46 See for example Lady Hale at para. 27 in *South Lanarkshire Council v Scottish ICO [2013] UKSC 55*

47 It is an unfortunate necessity of the DPA 2018 safeguarding ground that it is limited in its application to children (meaning those under 18) or adults with specific care needs, and so organisations that continue to have duties of care to individuals turning 18 may need to identify another legal ground to process relevant special category information about them. However, it may still be adequate if the sharing of information concerning an adult will have a protective function for others: especially where those others are themselves children who might come into contact with them.

48 Depending on the GDPR Article 6 condition relied on by the organisation to process the personal data: e.g. if the organisation is relying on consent that may be withdrawn; or if the processing is conducted under legitimate interests (in which case it must be balanced against any overriding rights or interests of the data subject).

49 Information Commissioner's Office (2019) *Special Category Data*, accessed on 25 November 2019 at https://ico.org.uk/media/for-organisations/documents/2616286/appropriate-policy-document.docx

(b) did not favour any requirement under long retention for regular historic file review, on grounds of "considerable additional burdens" to the "experienced child protection... workers" who are qualified safely to carry them out; and

(c) relevant to both points above, noted: "one of the primary reasons for retention is that information may take on a new significance in the light of later events".

26. Nothing in GDPR or DPA 2018 has changed the position since 2015 in terms of the principles of retention of personal data, or appropriate periods: the new law simply requires organisations to be more transparent and accountable in how this is done.

27. However, organisations lack guidance in understanding what categories of safeguarding record these principles apply to. Do they concern historic case files only; and/or records of low-level concerns, and/or allegations (i.e. that require referral to statutory agencies); or might (indeed should) they apply to other files and records retained for a primary safeguarding purpose but which do not record a low-level concern or an allegation?

28. Related to this question of what constitutes a safeguarding record, guidance is also lacking as to where low-level concerns should be recorded: whether as part of the ordinary child or personnel file; on the child protection or safeguarding file; or in a separate file (most likely still maintained by the Safeguarding Lead). In the context of schools and colleges, the question arises as to whether this would they fall within what should under KCSIE ordinarily be transferred on in the event a child moves schools.

29. Building from paragraph 25(c) above, it is a critical element inherent in records of low-level concerns that they may take on a new significance in the light of later concerns and/or events, and hence must be retained for long periods to have real value. This is the case whether or not the significance is immediately apparent; but any "just in case" retention policy needs to be weighed against:

(a) the possibility of relatively petty or prurient pieces of information being recorded, including by hearsay or through an excess of caution;

(b) the more tenuous relationship such information may have with the legal requirement of necessity set out above, particularly for individuals where no more concerning, problematic or inappropriate behaviours have manifested in the interim; and

(c) the likely discomfort and intrusion staff may feel in knowing that the information is being retained (whether self-reported or shared about them).

30. In addition to protocols (see paragraph 11 of the main guidance), records of low-level concerns may require layered retention periods. For example:

(a) records of low-level concerns as they relate to children (e.g. in a peer-on-peer risk context) or their parents might have limited value once the child has left the care of an organisation, and may come off the file, provided the Safeguarding Lead has taken a view about what needs to be shared with the Safeguarding Lead at the new organisation;

(b) low-level concerns about adults who work with children may continue to have relevance for the length of a working and/or volunteering life, and hence to future employers (etc.); but again organisations need to give careful consideration of whether to refer to any low-level concern in a reference – as discussed in the main guidance.

It is recognised that (a) is not the focus of this guidance, but it is anticipated that the principles may in due course have wider application to all areas of safeguarding practice.

31. We would recommend that, whenever staff leave an organisation (as well as considerations around the giving of references in paragraph 12 of the main guidance), the low-level concerns policy specifies that any record of low-level concerns that may be kept about such person is subject to specific review in terms of:

(a) whether some or all of the information contained within any record may have any reasonably likely value in terms of any potential historic employment or abuse claim so as to justify keeping it, in line with normal safeguarding records practice; or

(b) if, on balance, any record is not considered to have any reasonably likely value, still less actionable concern, and ought to be deleted accordingly.

Culture and Code of Conduct

32. The challenge of getting 'buy-in' from staff about the benefits and application of a low-level concerns policy is not only a necessity for proper practice and a happy and functional organisation, but also a GDPR Article 13 requirement under the transparency principle: data subjects (including staff, children and parents) must be provided with clear information about how their personal data will be collected and for what purpose, and how long it may be held.

33. Our experience is that, properly managed and communicated, staff typically see the benefits in self-reporting (as well as self-training and reflection), as well as the merit in a collegiate culture of sharing low-level concerns about peers where everyone understands the role they play in being watchful and responsible. To mitigate the risk of abusive or malicious sharing, as well as the pain of subject access, records must be fair and neutrally stated. This has to be approached culturally and in training for Safeguarding Leads and other staff.

34. We are further of the view that, even where an apparent concern is not found to be in breach of an organisation's Code of Conduct, this may not extinguish its value as a piece of potentially relevant safeguarding information. If so, it could still be kept on the low-level concerns file: if it is reasonably necessary, justifiable and relevant for a safeguarding purpose, the lawful basis to process it remains.

Data subject rights

35. It is one thing for an organisation to consult with its staff on and implement a low-level concerns policy. It is another to maintain the policy under the burden of data subject rights, in the event that staff object or require disclosure: single objection or erasure may undermine the record's value.

36. **Rights of erasure or objection**. This guidance is not the place for a detailed analysis of the available justifications for refusal; but the summary position with these rights is that they generally can, and therefore ought to be, resisted (as with any other type of safeguarding record) where low-level concerns are shared and recorded fairly and in good faith for a safeguarding purpose.

37. **Right of rectification**. The ICO takes a helpful position in terms of how organisations might deal with complaints about inaccurate information where accounts are disputed: for example, contemporaneous records, recorded in good faith, that might have value notwithstanding that the data subject disputes them. An ICO-approved response in such situations is to include a record of the data subject's objection, or contrary account, alongside the original record in a fair and neutral manner. This way its quality as evidence or information can be properly and fully assessed by those who come to review the file in the future.

38. **Subject access**. The existing ICO Subject Access Code of Practice has not been updated since the DPA 2018, but contains a note stating that it will be soon. It is to be hoped that among those new points considered will be the new Child Abuse Data exemption (see paragraph 39a below), along with issues for certain practitioners in an education, health or social services context concerning what is termed the "Assumption of Reasonableness" (see paragraph 46 below).

39. The subject access exemptions most likely to be relevant (albeit that they should not be assumed to apply in a blanket manner) are:

(a) the rule against needing to disclose confidential references;[50]

(b) the Child Abuse Data exemption,[51] where a person with parental responsibility has made the request on behalf of a person under 18 (with or without the child's authority, depending on the age and maturity of the child) but the personal data consists of information as to whether that child may be at risk of, has been or is subject to child abuse (widely defined to include sexual abuse, physical and emotional neglect, ill-treatment, and non-accidental physical injury) and the data controller deems that disclosure would not be in the child's best interests. However, this only applies in that narrow context (i.e. protecting a child as against a parent) and not more generally (e.g. to deny another adult access to their own personal data to protect a child);

(c) if the matter concerns education, social services or medical data[52] and disclosure risks "serious harm" to any individual (a high bar);

(d) where the organisation performs certain functions designed to protect the public (e.g. from seriously improper conduct or unfitness; or where those at work may pose a risk to the health or safety of other persons), but only where disclosure is likely to prejudice the proper discharge of that function;[53] and

(e) if any third-party privacy rights[54] can be argued (notably those of the child) – but only to the extent they would be identifiable in relation to their own personal information in the particular record concerned, by context or otherwise. In other words, this exemption

50 Paragraph 24 of Part 4 of Schedule 2 DPA 2018
51 Paragraph 21 of Part 5 of Schedule 3 DPA 2018
52 See throughout Parts 3 and 4 of Schedule 3 DPA 2018
53 Paragraph 7 of Part 2 of Schedule 2 DPA 2018. Please note this exemption is not easily applied to all organisations with safeguarding responsibilities: they need not be public bodies, but the function must be of a public nature and in the public interest. It is also the ICO's view, although this is nowhere in statute, that the function should be the core activity of the organisation (i.e. regulatory in nature), and that the exemption should not be used to protect internal grievance, complaint or disciplinary functions.
54 Paragraph 16 of Part 3 of Schedule 2 DPA 2018. Please note this would be of no application if only the adult himself/herself was identifiable from the record, or part thereof, even if there was concern for the safety of a particular child or children. Any separate personal data of the adult would be disclosable.

could apply if more than one person's data could be inferred from how a low-level concern is recorded (even if not explicitly named), unless it were still reasonable in all the circumstances to disclose their personal data to the requester.

40. Contrary to widespread belief in some quarters, however, there is no general "safeguarding record" exemption that could be used to protect records about staff from access by those staff members. Nor, as set out in paragraph 7 of the main guidance, is this in our view needed, for the following reasons:

(a) information that could identify specific children should not be disclosed to staff making subject access requests, and this is quite lawful to withhold under existing rules;

(b) similarly, the identity of the person sharing the low-level concern could also be withheld under subject access, if they have not given their consent to their own data being disclosed to the requester and it is not otherwise reasonable to do so (although it may necessarily emerge in the context of a procedure or claim under employment law). This may not be straightforward, however, if it is likely to be clear in context who shared the low-level concern. The issues here should be made clear in the low-level concerns policy, and may be for the Safeguarding Lead to discuss with the person sharing the low-level concern; and

(c) in our view, the policy reasons in favour of transparency with affected staff about low-level concerns – as well as the need for such concerns to be fair, accurate and (where appropriate) raised directly with the person in question – tend to outweigh any benefits of "covert" recording.

41. If the low-level concerns policy is operating properly, then its contents under a subject access request should not come as a surprise to the person about whom such a concern has been recorded. There may be a risk that a request is made before a low-level concern has been adequately raised with the adult in question: but, as long as the order of things is consistent with the applicable policy, then the controller will be able to make the case for the actions taken.

42. Organisations should not feel unduly burdened by introducing policies intended to assist in the protection of children. This is best approached by transparency, training, and a careful approach to sharing low-level concerns (as also discussed in the main guidance). Equally important, from an employment perspective (both in terms of process and staff trust), is providing clarity about how this information may be used. Collection of such data must be transparent and raised with individuals so that, if necessary, it can be challenged.

43. Properly managed, a low-level concerns policy should not substantially increase the volume burden in subject access. But it is also our experience that, beyond the purely administrative burden, there may be a reluctance to share due to the embarrassment and distress (both to individuals and controllers) that a low-level concerns policy may cause, risking unwarranted reputational damage to individuals. In some organisations this understandable fear may have a chilling effect on the sharing and recording of low-level concerns.

44. However, subject access can fairly be viewed as a necessary form of checks and balances for data controller organisations to record such information fairly and neutrally. Despite the considerable burdens on organisations caused by subject access, there is a strong privacy interest in supporting this right, protected (for the time being at least) in UK law as a fundamental right under Article 8(2) of the Charter of Fundamental Rights of the European Union (EU Charter). The more impactful and personal the information, as here, the greater the need for organisations to be accountable to affected individuals.

45. **Children's rights of access or erasure**. The main guidance focuses on sharing low-level concerns about adults' behaviour towards children, not on concerns being raised about children in a peer-on-peer context, or in assessing their vulnerability. However, should identifiable data about specific children be contained in information held in a record of a low-level concern about an adult's behaviour towards them:

(a) this is something the controller may withhold in respect of a request made by the adult in question; but

(b) this could be disclosable upon request by that child or (depending on age, circumstances, and the child's best interests) someone with parental responsibility for the child.

46. It is worth noting that, in a schools context,[55] the DPA 2018 "Assumption of Reasonableness" has the effect that personal data of staff should not be

55 As well as in other contexts around social care and health. However, this rule currently lacks clarity and should perhaps be treated with caution pending further case law or commentary by the ICO.

anonymised or withheld under a subject access request made by or on behalf of a child in their care, where it would otherwise be disclosable under that child's subject access rights.[56]

47. For this reason, where possible, and unless this would diminish its safeguarding value, low-level concerns recorded as against an adult should be recorded separately from identifying details of the child if organisations (not limited to schools) believe that the staff member in question should fairly and safely be protected from access to their low-level concerns record by parents or pupils.

48. **Data Security**. GDPR more generally requires that data controllers have security measures (both technical and organisational) that are appropriate to the nature of the data and processing. The most critical aspect, given the highly sensitive and potentially damaging nature of the information contained in even low-level concerns, is to maintain and enforce a need-to-know-only access policy. Aside from any rights of access by individuals about whom concerns have been reported (as above), this would be limited to appropriate, trained persons with a specific and appropriate role in the safeguarding team or – potentially – those providing human resources or legal support, where lawful and necessary.

49. All controllers are not alike in resources, but the affordability of readily available password protection and encryption software means that the digital retention and, where necessary, onward sharing of such information should be made adequately secure. Such steps should already be in place for allegations reporting. Within the low-level concerns policy itself, thought must be given to the most appropriate and secure means of sharing concerns by staff with the Safeguarding Lead, or with a values guardian/safeguarding champion, without making it sufficiently difficult as to discourage reporting or self-reporting.

50. This may best be carried out by means of a face-to-face meeting (see paragraph 8.18 of the main guidance), whether or not supported by a form such as that at **Appendix E**. That way, control and oversight of record-keeping can remain with the Safeguarding Lead. When a policy permits forms or concerns to be submitted (by whatever means) remotely, or in total anonymity, this raises more practical challenges in maintaining appropriate levels of security for organisations to consider. Electronic submissions, for example, would be better handled via a secure portal and not by allowing concerns or forms to be transmitted by – or worse, remain on – general email servers.

56 Paragraph 7 of Part 3 of Schedule 2 DPA 2018: this is the rule that there should be a starting assumption that school staff, health workers and social workers can expect no rights of privacy under subject access. However, the limits on its application are unclear and – absent ICO guidance – there is the risk that its literal interpretation would lead to inadequate protection of the rights of these adults.