PE1692/C
The Information Commissioner's Office submission of 31 July 2018

Thank you for your letter of 3 July, inviting the Information Commissioner's Officer (ICO) to provide its views on the action called for in the above petition.

Unfortunately, the petitioners' proposed action calls for an Inquiry into the human rights impact of Getting it Right for Every Child (GIRFEC) and the Information Commissioner's Office (ICO) has no locus in respect of this legislation. As such, I am afraid that I am unable to comment on the merits or otherwise of the action itself. However, having read the Official Report of the Committee meeting of 28 June and the background information on the Petition itself, I note that the discussion is much wider than human rights and also brings in issues of data protection. As the Regulator of the data protection regime in the UK, I am happy to provide input to the Committee's deliberations from that perspective.

Fundamentally, the issue under question is the sharing of personal information between organisations for the purposes of the Scottish Government's GIRFEC initiative. GIRFEC introduced the concept of wellbeing into children's services and it is the petitioners' view that personal information shared without consent for wellbeing purposes is inappropriate at best and perhaps unlawful in some cases. I think it might be helpful for the Committee to understand how data protection legislation is relevant to the sharing of personal information.

The law in place at the time of GIRFEC's introduction was the Data Protection Act 1998 (DPA 1998). In May 2018, the vast majority of this Act was repealed and replaced by the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA 2018). Under both the old and the new regimes, the preamble to the EU legislation from which they are derived, provides for *the protection of individuals/natural persons with regard to the processing of personal data* ***and the free movement of such data*** (Directive 95/46/EC & Regulation (EU) 2016/697). They essentially provide a framework for the use, including sharing, of personal information.

The first Data Protection Principle in both regimes is broadly similar in that:

> Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject [the individual to whom the data relate] (GDPR Art5:1(a))

In terms of lawful processing, this has two aspects that must be met. First, for the processing to be lawful it must rely on specified legal bases as set out in the data protection legislation. Second, it must not contravene any other legislative

requirement. As the latter is self-evident, I shall confine my comments to the former.

Schedules 1 and 2 of the DPA 1998, set out the legal bases for the processing of personal and sensitive personal data respectively, the first of which in both cases is consent (explicit consent for sensitive personal data). The rest of the legal bases provide for situations where it would be unreasonable or inappropriate to rely on consent because the processing is considered to be *necessary* for one of the specified lawful purposes, such as *to protect the vital interests of the data subject*. This legal basis could be relied on, for example, to share information where there is potential for significant harm, i.e., a child protection issue. If personal information is to be shared without consent at a level below the vital interests/significant harm bar, the organisation in question must be able to rely on one of the other legal bases such as it being *necessary for the exercise of any other functions of a public nature exercised in the public interest*. For this to be lawful, the organisation must be able to identify the public function in question, usually, but not exclusively, set out in statute, and the sharing must relate to that function.

It is important to note that all legal bases carry equal weighting with none more or less valid than any other. Consent, therefore, is not the only legal basis for the lawful sharing of personal information between organisations. However, where consent is not being relied on, the organisation must be prepared to justify its position clearly.

Under the new data protection regime, the same requirements apply and organisations engaged in the sharing of personal data since 25 May 2018, must be able to rely on one of the legal bases set out in GDPR/DPA 2018. The matter of consent, however, is more problematic for public authorities under the new regime. The GDPR provides for a more robust consensual process, the focus of which is that is must be meaningful and individuals must have real choice in the matter so that, should they wish, they can withhold or withdraw that consent with no real detriment. For public authorities, this is especially difficult because of the inherent nature of the relationship between it and its constituents. As Recital 43 of GDPR articulates:

> In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, **in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation**. (added emphasis)

Given the nature of the relationship between public authorities and children, young people and their parents/guardians, the potential for an imbalance is exceedingly high. Indeed, the potential for such was implied at paragraph 95 of the Supreme Court Judgment where it states that:

> …there must be a risk that, in an individual case, parents will be given the impression that they must accept the advice or services which they are offered…and further, that their failure to co-operate…will be taken to be evidence of a risk of harm. ([2016] UKSC 51[1])

The GDPR's more robust regime around reliance on consent substantiates fully the consistent position the ICO has taken on the matter in that consent should only be relied on when individuals have real, meaningful choice. If sharing is deemed necessary regardless of consent, one of the other legal bases must be used and organisations must be prepared to justify their position.

It would be remiss of me not to mention that the DPA 2018 now provides a specific legal basis for the necessary processing of special category (sensitive personal) information for the Safeguarding of children and of individuals at risk (Schedule 1:18). However, caveats ensure that this is not used for wholesale sharing but only that which meet the specific circumstances outlined in the provision.

The second part of the first Data Protection Principle is the concept of fairness and transparency and this permeates every aspect of data protection compliance. This is about ensuring that individuals are fully informed about how their personal information is to be used. Again, the new regime is much more robust in this requirement and introduces a fundamental right to be informed and requires that more detailed information is provided, including where the information was obtained – if not from the individual themselves - and with whom information will be shared. As I said, this is fundamentally important because even if the sharing is deemed necessary and consent is not being relied on, the processing will be unlawful if individuals have not been fully informed about how their information is to be used. Of course, there are exceptions to this but the overriding imperative of data protection is transparency so they should only be used when absolutely necessary. For example, it would be wrong to inform an individual about any specific processing where to do so would be prejudicial to the purposes. However, this notwithstanding, it is vital that public authorities get this right because it is an important part of mitigating that imbalance.

---

[1] The Christian Institute and others v The Lord Advocate (Scotland) 28 July 2016

Regardless of whether the legal basis for sharing is consensual or necessary, it is very definitely about proportionality: sharing only that which is absolutely necessary with the relevant person at the appropriate time. This speaks to the third Data Protection Principle and, again, the ICO has been consistent in saying that the sharing of personal information must be adequate, relevant and limited to what is necessary for the purposes.

Ultimately, it is for each organisation to justify its reliance on any given legal basis and if young people/parents/guardians believe that such reliance is erroneous, provided they have exhausted organisation's complaint process, they can raise the matter with the ICO.

I trust that the Committee find this helpful in its deliberations.