Upholding information rights

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

Eilis McDaniel
Family and Children's Policy Directorate
Department of Health
Room A3.3
Castle Buildings
Stormont
Belfast
BT4 3SQ

By email only: eilis.mcdaniel@health-ni.gov.uk

13 November 2020

Dear Ms McDaniel

Re: CONSULTATION ON CROSS-DEPARTMENTAL COVID-19 VULNERABLE CHILDREN AND YOUNG PEOPLE'S PLAN

Thank you for your email regarding the Department of Health's (DoH) consultation on the Cross-Departmental Covid-19 Vulnerable Children and Young People's Plan.

We have reviewed the consultation document and have provided some comments below which we hope will be useful in your cross departmental planning for this area. Our comments are being raised as general considerations for the DoH and other involved stakeholders to consider in the development of any potential strategy going forward.

Data sharing

Within the "Actions" category on Page 5 of the consultation document, we note the proposal that "Children's services continue to investigate and respond to child protection concerns and services/agencies continue to work collaboratively, sharing information/concerns appropriately". In addition to this, page 10 of the consultation document refers to "the Working through public health restrictions to continue to ensure appropriate sharing of information/concerns between statutory agencies."

Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510

It is important to ensure that when contemplating the sharing of children's personal data, the best interests of the child is a primary consideration. Furthermore, when sharing children's personal data with third parties or with other parts of your own organisation, you should be satisfied that it is fair to the child to do so. Sharing children's personal data with third parties, including sharing data inferred or derived from their personal data, can expose children to additional risks which go beyond those inherent in an organisation's own processing.

Personal data should not be shared if it can reasonably be foreseen that doing so will result in third parties using children's personal data in ways that have been shown to be detrimental to the child's wellbeing. Ultimately, it is up to the third party you have shared the data with to ensure they comply with the requirements of the GDPR (in their role as a data controller for the personal data they receive). However, you are responsible for ensuring that it is fair to share the personal data in the first place. You should not share personal data unless you have a compelling reason to do so, taking account of the best interests of the child. It is important to obtain assurances from whoever you share the personal data with about this, and undertake due diligence checks as to the adequacy of their data protection practices and any further distribution of the data.

Appropriate data sharing arrangements and procedures should be in place to ensure data sharing is carried out in line with the legal data protection framework. We will shortly be publishing our revised Data Sharing Code of Practice which you will be able to find here on our website.

Lawful basis

When organisations are contemplating data sharing, they must ensure that they have identified a lawful basis for processing the relevant data.

Given the nature of the information that is proposed to be shared between the various bodies listed, it is possible that some of the personal data may be deemed special category data. Furthermore, references are made to the PSNI and Youth Justice Agency which suggests that criminal offence data may also be shared.

With respect to the processing of criminal offence data, organisations must ensure that they have a lawful basis for the processing of personal data under

Article 6 of the GDPR while also complying with the requirements of Article 10 of the DPA 2018. This means that organisations must either:

- process the data in an official capacity; or
- meet a specific condition in Schedule 1 of the Data Protection Act 2018, and comply with the additional safeguards set out in that Act.

More information on the requirements above is available here on our website.

With respect to the processing of special category data, such as health/social care information, organisations must ensure that the processing undertaken is lawful. To ensure that processing special category data is lawful, organisations must be able to rely on an Article 6 basis for the processing and be able to meet one of the specific conditions in Article 9 of the GDPR along with the relevant DPA 2018 provision if required. Further information regarding the processing of special category data can be found here.

Digital solutions and online services

Within the "Actions" section on Page 8 of the consultation document, reference is made to:-

"Digital solutions, including apps and page tracker, are being utilised where possible to ensure allied health professional therapy advice and online guidance is available for families"

Furthermore, the "Actions" section on page 5 discusses the "Ability for young people to connect with youth worker via 'Youth Online' – a platform where young people can access 'Stay Connected' service."

On 2nd September 2020, a new statutory code (Age Appropriate Design Code, sometimes referred to as the ICO children's code) was introduced which requires organisation's to provide better online privacy protections for children. The code is currently within its 12 month transition period which is aimed at affording organisations an opportunity to takes measures to ensure compliance.

The code sets out 15 standards for designers of online services and products and how they should comply with data protection law. The code applies to 'information society services' likely to be accessed by children in the UK. In

simple terms, that means many apps, online games, connected toys and devices, search engines, social media platforms and websites that offer goods, news or education services.

Given the nature of some of the online services/apps being proposed, which may encourage use by individuals under the age of 18, consideration should be given to ensuring the principles outlined within the children's code are reflected in the design and operation of solutions and services being proposed. You can read more about the ICO children's code here.

Furthermore, as with any project which requires the processing of personal data, organisation's should consider carrying out a Data Protection Impact Assessment (DPIA) prior to project launch. A DPIA will help an organisation to identify and minimise any associated data protection risks emanating from a particular project. DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage and the potential for harm to individuals.

DPIAs are a legal requirement for processing that is likely to be high risk. An effective DPIA can bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals. Where an organisation has identified high risk processing and is unable to mitigate the risk, it must consult with the ICO. Further information about DPIA's can be found here.

Security, data minimisation and retention periods

Within the "Actions" category on page 11 of the consultation document, reference is made to the:-

"i. Collection of information daily relating to children in schools.
iii. Gathering and using intelligence from a range of sources, including advice lines and hub referral trends, to identify any emerging issues and inform strategy and decision making."

Given the sensitive nature of the personal information being collected, specific and detailed consideration should be given to ensuring appropriate security measures are implemented so that personal information is not compromised. The completion of a DPIA may assist with identifying any potential risks associated with proposed personal data processing projects. As part of this, organisations

should consider areas such as cyber security, human error data breaches, inappropriate access to sensitive information, staff training, data storage and data transfer mechanisms. Article 25 of the GDPR mandates that, at the time of the determination of the means of processing and at the time of the processing itself, appropriate technical and organisational measures should be in place to implement data protection and to integrate the necessary safeguards into the processing.

It is important that organisations give consideration to the GDPR principle of data minimisation. Organisations must only process **the minimum** amount of personal data required to fulfil its purpose. They must also review their processing regularly to check that the personal data held is still relevant and adequate for its documented purposes. Organisations must not retain personal data for longer than is required. They should be able to justify the retention period and ensure that any personal data that is no longer needed is deleted accordingly.

We would be happy to engage further with you in respect of any strategy developed by the DOH as a result of this consultation. Additionally you may find useful information within our coronavirus information hub platform which is regularly updated and designed to assist individuals and organisations to navigate data protection issues during this unprecedented time. In the meantime, we hope you find the above comments helpful.

Yours sincerely,

Caroline Mooney
Regional Manager
ICO (Northern Ireland)