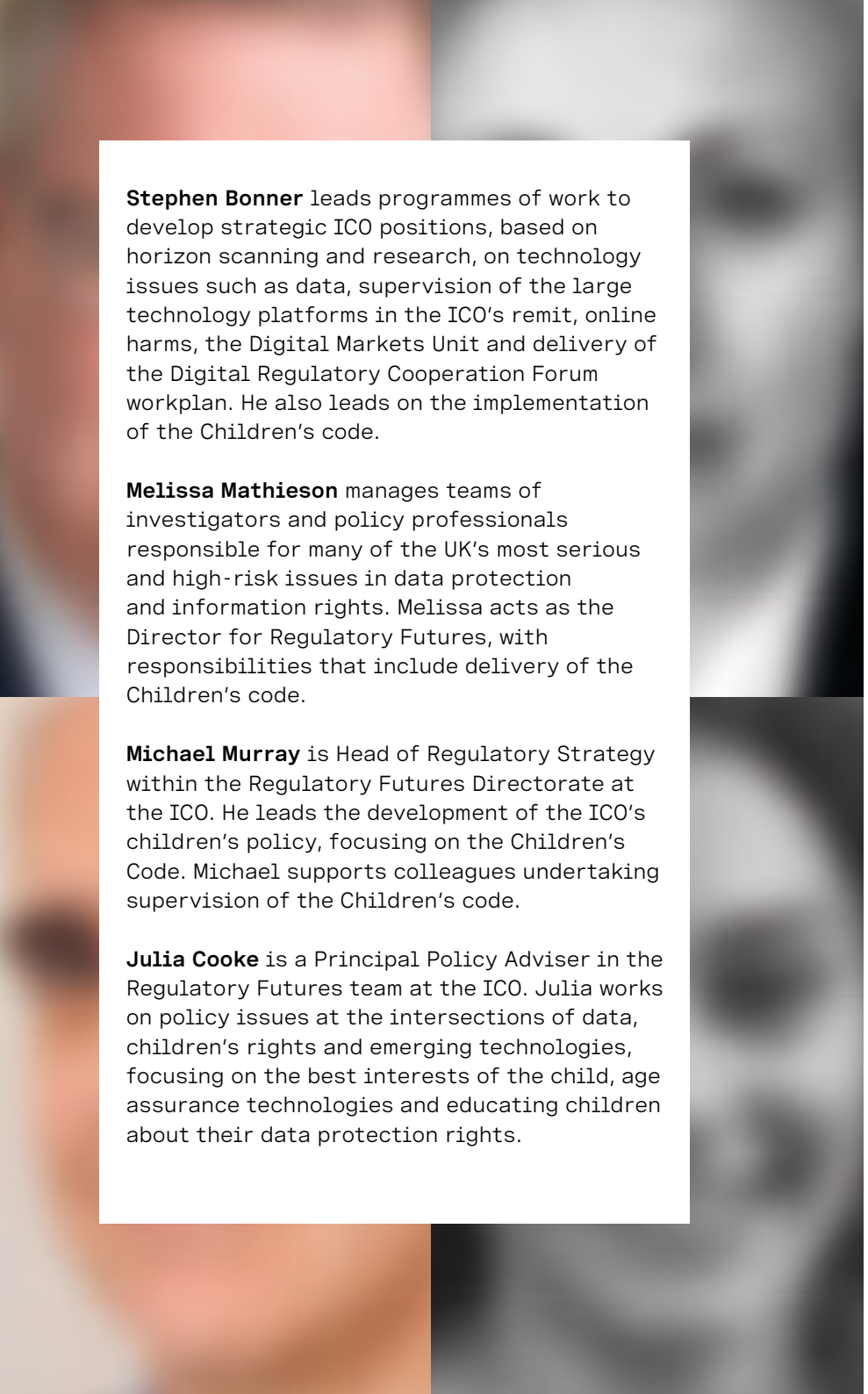

Stephen Bonner leads programmes of work to develop strategic ICO positions, based on horizon scanning and research, on technology issues such as data, supervision of the large technology platforms in the ICO's remit, online harms, the Digital Markets Unit and delivery of the Digital Regulatory Cooperation Forum workplan. He also leads on the implementation of the Children's code.

Melissa Mathieson manages teams of investigators and policy professionals responsible for many of the UK's most serious and high-risk issues in data protection and information rights. Melissa acts as the Director for Regulatory Futures, with responsibilities that include delivery of the Children's code.

Michael Murray is Head of Regulatory Strategy within the Regulatory Futures Directorate at the ICO. He leads the development of the ICO's children's policy, focusing on the Children's Code. Michael supports colleagues undertaking supervision of the Children's code.

Julia Cooke is a Principal Policy Adviser in the Regulatory Futures team at the ICO. Julia works on policy issues at the intersections of data, children's rights and emerging technologies, focusing on the best interests of the child, age assurance technologies and educating children about their data protection rights.

Data protection - a framework for sharing children's data in their best interests

Stephen Bonner, Melissa Mathieson, Michael Murray and Julia Cooke, Information Commissioner's Office

The Information Commissioner's Office (ICO) has long advocated data sharing that supports children's best interests and the benefits that timely data sharing can bring.† As the UK's regulator for data protection, the ICO is uniquely placed to provide insights gathered through supervision of the legislation and policy engagement.‡ This is our opportunity to demonstrate why data sharing is important and how to do it well, but also to discuss the improvements needed to ensure data sharing supports children's best interests. We advocate a framework for sharing children's data that balances the risks of sharing data (such as excessive, inappropriate sharing) with the risks of not sharing data (such as not being able to make informed decisions or effectively act on crucial information). Such a framework would enable children to experience benefits including improved access to services, targeted help and support, and better projected and actual life outcomes (ICO, 2020a, b; National Infrastructure Commission, 2017).

† The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

‡ The ICO's policy engagement spans all sectors and industries that process children's data, from health, social services, education, central and local government to recreational and online services. It has undertaken research to inform these recommendations, including with parents, caregivers and children (ICO, n.d., a, b). It also funded research led by Professor Sonia Livingstone on children's data and privacy online (ICO, n.d., c).

Step-change in children's digital footprints

Personal data powers innovative technologies and online commerce. With many of us now leading the majority of our daily lives online, personal data quantifies our behaviour, our interests, our spending patterns, our loves and likes, our beliefs, our health, sometimes even our DNA – the very blueprints that make us who we are. However, any economic and societal benefits from sharing data are only sustainable if people have confidence and trust in how their data is used. This is never more so than when considering the interests of children and vulnerable people.

In 2003, only half of UK homes were connected to the internet (Ofcom, 2021). By 2021, Ofcom (2021) found that 97 per cent of all children aged 5–15 went online. This step-change in digital usage has accelerated concerns about protecting personal data, especially when children are creating digital footprints and sharing data from a young age that follow them into adulthood on a scale previously unseen (Lupton & Williamson, 2017). The rise in online learning, including automated decision-making and artificial intelligence (AI)-powered teaching aids, as a consequence of the COVID-19 pandemic, has further exacerbated these concerns.

The internet was not designed for children's use or with their best interests in mind. Children can be unaware of the impact sharing their data has, as seen with prominent celebrities facing repercussions for comments they made as children (Ritschel, 2019; Watson, 2021). As well as having less understanding of how their data is used and what their rights are, the unequal power differential between organisations and data subjects means children are often less empowered to complain about misuse of their personal data, and frontline, child-focused services are often unaware of how data collected on children by digital service partners can be shared with third parties. It is imperative that we protect and educate children within the digital world, and ensure all stakeholders are aware that data protection is fundamental to supporting children's rights and making the internet, and data sharing, better for children.

The legislative framework

The UK's data protection regime, comprised of the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018, creates a framework that enables child-centric, fair, necessary and proportionate data sharing to take place in a way that safeguards children and supports their best interests.† The ICO has developed two statutory codes of practice to support organisations in sharing children's data lawfully: the Data Sharing Code of Practice (ICO, 2020b), which includes a section specifically focused on sharing children's data (ICO, 2020d), and the world-leading Children's Code (Age Appropriate Design Code; ICO, 2020e). The success of the Children's Code has caught the attention of other countries, which are now looking at changes to their legislative frameworks, as seen in Ireland with the Fundamentals, in the Netherlands with the Code for Children's Rights and most recently, in the USA with the California Age Appropriate Design Code Act.

The Data Sharing Code of Practice helps organisations balance the benefits and risks in order to implement successful data sharing. It demonstrates that the legal framework is an enabler to responsible data sharing, and busts some of the myths that currently exist. Organisations can use it to guide them through each step of the data sharing process (ICO, 2020c). For example, the ICO's Innovation Hub provided advice and guidance to an organisation designing solutions that used Open Banking to divert a small, adjustable portion of income into a hidden account, in order to increase women's financial independence and empowerment.‡ This data sharing focused

† The UK Government is reviewing the data protection regime to ensure it is fit for purpose and underpins the trustworthy use of data (see DCMS, 2021). The ICO welcomes this opportunity to review the state of play three years on from the introduction of the GDPR to ensure the framework continues to support data sharing in children's best interests. Organisations are encouraged to engage with this review, and the ICO has published its response (ICO, 2021a). This demonstrates the ICO's support for proportionate ways organisations can demonstrate their accountability for how they collect, store, use and share data. Organisations must ensure data is safe and not used in ways that might cause harm, that all people, including children, are able to exercise rights over their personal data.

‡ Open Banking (www.openbanking.org.uk) enables customers to allow organisations to receive data directly from their bank with their explicit consent (FCA, n.d.). Research has previously found that 60 per cent of women in refuges had children with them, so using Open Banking to share data in this instance has the potential to support children in households experiencing domestic abuse by financially enabling them to flee violence and the known negative impacts of living in a home with domestic violence (NSPCC, 2021; Women's Aid, n.d., 2022).

on enabling customers in controlling or abusive relationships to retain some financial independence, as finance is a key barrier cited by victims that prevents them from leaving (Butt, 2020; Women's Aid, 2022).

What does 'good' data sharing look like?

Too often, harm and detriment are caused to children where data is not disclosed for fear of breaching data protection, is shared too slowly or without due consideration of the risks, potentially rendering the sharing ineffective, or the data biased or inaccurate, leading to flawed decision-making.[†] Data protection helps organisations to confidently share data correctly, efficiently, safely and in support of children's best interests.

Successful data sharing:

- Is underpinned by a data protection impact assessment (DPIA)
- Takes a child-centric, holistic approach
- Builds on existing best practice
- Involves collaboration with other parties.

DPIAs

Organisations can use DPIAs to identify and minimise the data protection risks of any processing operation. Article 35 of the UK GDPR specifies several circumstances where it is necessary for organisations to complete DPIAs, including where there is large-scale processing of special category data, which includes children's data (ICO, n.d., d). Standard two of the Children's Code requires organisations to complete DPIAs in order to process children's data.[‡] It is a living document rather than a one-off process, and should be regularly reviewed and updated. For example, having an emergency plan in place that considers data sharing can help prevent any delays in a crisis and get children the emergency support they need (ICO, 2021b).[§]

† Such harm and detriment can range from not receiving care and support, emotional distress, unwarranted intrusion on families or discrimination to loss of life in extreme cases; see DfE (2016).

‡ See the ICO's DPIA template (ICO, 2020h).

§ Schools should also have plans in place for emergencies, as outlined in DfE (2018).

Child-centric holistic approach

The United Nations Convention on the Rights of the Child (UNCRC) recognises that children need special safeguards and care in all aspects of their life, and that these should be guaranteed by appropriate legal protections (UN OHCHR, 1989). In the UK, the Children's Code ensures domestic data protection laws truly transform the way children are safeguarded when they access online services. This means that the best interests of the child are a primary consideration when designing and offering services to children.

The ICO has developed a framework to assist industry to apply the principles of the UNCRC, so they can demonstrate their decision and justification for processing personal data, their consideration of risks and measures to mitigate any risks identified (ICO, n.d., e). If these considerations are not undertaken, it's likely their processing will not be in compliance with data protection and will not be considering the best interests of the child. This framework can be integrated into DPIAs and organisations empowered to substantively and holistically centre children in their considerations. Open sharing of children's data that is child-centric and takes a holistic approach that enables early intervention (ICO, n.d., f) highlights the need for a culture that supports and facilitates appropriate data sharing for early intervention and how to practically implement this, such as clear, designated points of contact for sharing.

Promoting the best interests of the child aligns with schools' educational role. They must comply with data protection legislation, and the Children's Code sets out what good practice compliance looks like in the areas it covers. All organisations should be encouraged to meet the Code's standards as a matter of general good practice. Doing this will ensure the schools' and their digital services providers' processing of personal data centres on the child's best interests and supports their learning.

Build on existing best practice

When creating data-sharing systems, organisations should build on existing best practice examples. This will enable data sharing that is safe, secure and timely, in line with the highest

possible standards. For example, the Welsh Government-funded Wales Accord for Sharing Personal Information (WASPI) provides a toolkit for data sharing to support delivery of frontline services by the public sector and other partners.[1] One of the principles of WASPI is that quality-assured information-sharing agreements are published so other partnerships can refer to them when developing similar proposals. Data sharing through WASPI also supports coordinated delivery of services for children and teenagers with special needs, and for those who may be at risk of neglect, abuse, exploitation by criminals or radicalisation, and those who have gone missing.

Multistakeholder approach

A multistakeholder approach has several benefits for children that can lead to a joined-up offer that better supports different aspects of a child's life. In a child welfare context, this allows specialist services to investigate potential harm and put in place tailored support for children that is appropriate to their individual needs. It can also reduce gaps in knowledge that could lead to a risk of harm to a child, and increasing the efficiency of sharing data.

The ICO engaged with the Northern Ireland Department of Justice on new Regulations to safely facilitate the sharing of personal data in relation to incidents of domestic violence.† These Regulations, which came into force on 1 April 2022, enable early intervention safeguarding to support children and young people experiencing domestic abuse. They enable schools to provide immediate support to impacted pupils and support their best interests. This initiative includes multiple stakeholders, including the Education Authority, the Police Service of Northern Ireland, the Safeguarding Board of Northern Ireland and a number of nurseries and schools, empowering them to share data to support children and minimise negative impacts on them.

Organisations need to demonstrate effective accountability and transparency, ensure the accuracy of data and work to increase confidence and trust in how they share data.

Accountability

The UK GDPR accountability principle means that organisations must be able to demonstrate how they comply with the law, including by demonstrating how their data sharing is proportionate to the risks to children associated with the data sharing (ICO, n.d., g). For example, organisations must:

- Complete a DPIA for sharing children's data
- Have contracts or agreements in place that define the responsibilities of the various organisations
- Detail the lawful basis for processing and sharing data
- Provide privacy information to children about how their data is used

In 2020, the ICO audited the Department for Education (DfE), focusing on their use of data compiled into the National Pupil Database (NPD).† This audit did not find any instances where data protection legislation impeded data sharing or placed barriers on the use of data in the public interest, although it did identify risks arising from data sharing without sufficient controls.‡ There was limited oversight and consistency around how data was shared externally, with no formal, consistent assessments carried out about the purpose, legal basis and risks of sharing the data.§ For example, only 12 instances of data sharing were rejected out of 400 applications, largely because the data-sharing process was designed to find a legal gateway to 'fit' the application, rather than a holistic assessment of the application against a set of robust measures designed to provide assurance and accountability that the sharing was lawful and in line with statutory requirements.

In a similar but separate instance, a lack of controls was a key concern with how the police and local councils processed

† The Domestic Abuse Information-sharing with Schools etc. Regulations (Northern Ireland) 2022 (NI) (UK). See also Campbell (2022). These are modelled on existing regulations that have been in place in England for over 10 years, and demonstrate the value of adopting best practice.

† This is not a database in its own right, but is made up of links to various other databases or collections of data, including the school census, the Early Years Foundation Stage Profile (EYFSP) and Children In Need census (CIN). See DfE (2022) and ICO (2020f).

‡ These risks included data sharing that was not in compliance with data protection legislation, which is a risk to the data subjects, who, in this instance, are children, and also the data controller.

§ For further information, see ICO (2020g).

and shared information on young people suspected of being involved in gang violence. Data was inappropriately shared with several organisations, resulting in the withdrawal of services and opportunities. Many individuals were under 18 and not all were accused of any crime, but rather, some were victims of crime. This case illustrates the need for an organisation to demonstrate accountability when it shares data, and to have sufficient policies and protocols in place to enable proportionate, secure and accurate data sharing in the public interest (ICO, 2020b).

Data minimisation

Organisations must apply data minimisation to their processing, including data sharing. This means data must be adequate, relevant and limited to what is necessary. UK GDPR requires organisations to:

- Be clear about the purposes for which they collect personal data
- Only collect the minimum amount of personal data needed for those purposes
- Only store that data for the minimum amount of time required

Data minimisation is a central concern around children's data, as seen with moves to use biometric data in schools to facilitate the provision of services, in particular the use of facial recognition technology to enable contactless payments for school lunches (BBC News, 2021). To comply with data minimisation, organisations should use the least intrusive measure available to achieve the processing goal, and should consider whether any use is necessary and proportionate prior to processing.

Better transparency and education

Transparency is fundamental to people's trust and confidence in how their data is used; it is a crucial foundation for successful data sharing. However, transparency is often absent, especially in schools, leaving people in the dark about how children's data is being shared. Coupled with a lack of education around the use of their data, this can leave children or their parents or caregivers disempowered, unaware of and unable to assert their data protection rights.

A 2018 review of the 1200 highest ranked apps targeted at children from the Google and Apple app stores found the average reading age for privacy policies was 13 - four years above the average reading age for an adult in the UK of nine (Das et al., 2018). Lack of transparency is therefore of particular concern when it comes to processing children's data. Children can be less aware of the risks involved in their data being processed and shared, and this can impact them in ways they don't expect (Wang et al., 2019). The ICO has published school resources for teachers to use when educating children about personal data and how it is used.[2] These empower children to know their rights and how to assert them.

The ICO recently called for transparency champions to find good practice in providing accessible, easy to understand transparency information to children (ICO, 2021c). This produced five recommendations:

1. Be creative with format - but avoid style over substance
2. Put children's needs and views at the heart of the design process
3. Meet children and parents where they are
4. Unbundle privacy information for engagement and understanding
5. Create space for meaningful parent-child conversations

Organisations should embed these recommendations into their approach to sharing children's data, and tell children about this in order to improve trust and confidence in their data sharing.

Increased confidence in sharing data

It is crucial that organisations develop a culture whereby staff feel empowered to share data safely, but to do this, staff need to have received appropriate training.

An ICO audit of Multi Academy Trusts (MATs) (ICO, n.d., h) found that 70% did not include training for all staff on key areas such as data protection, data sharing or requests for personal data. Forty per cent either hadn't allocated adequate resources to deliver such training or staff had not received appropriate training in order to train other staff (ICO, n.d., h). One organisation directly provided training to all staff, including temporary and contract staff such as supply teachers. This ensured all staff had the same level of training and awareness in order to successfully share data in ways that complied with data protection and supported children's best interests.

The 2011 Munro review of child protection highlighted that to ensure the sharing of data to support children's best interests, we need to move towards a child protection system with 'greater trust in, and responsibility on, skilled practitioners at the frontline' (Munro, 2011). The UK Government's 2018 information sharing advice for practitioners reaffirms this, highlighting that for data sharing to be successful, practitioners should be confident about the processing conditions. It starkly notes that 'poor or non-existent information sharing is a factor repeatedly identified as an issue in Serious Case Reviews (SCRs) carried out following the death of or serious injury to, a child. In some situations, sharing information can be the difference between life and death' (HM Government, 2018). The ICO's Data Sharing Code of Practice emphasises that 'sometimes, it can be more harmful not to share data' and includes case studies where data sharing is needed, particularly in relation to vulnerable children or safeguarding purposes.

Standard 9 of the Children's Code notes that organisations should not share children's data unless they can demonstrate a compelling reason to do so, taking account of the best interests of the child. As there is some confusion about what might constitute a compelling reason to share data, the ICO has explicitly highlighted examples in the Data Sharing Code of Practice. For example, data protection law does not prevent data sharing that is necessary to prevent serious harm to a person, prevent the loss of human life or the effective safeguarding of children.

Accuracy and rights related to automated decision-making

Finally, any decision or action taken is only as good as the data it is based on, so data must be accurate.† This means that data is not only up to date, but also impartial, with any bias sufficiently mitigated (ICO, 2020i). Research highlights the long-lasting impact that follows children into adulthood when personal data is incorrectly, or insensitively, recorded in health and social care files, so it is imperative that data is recorded accurately, particularly when sensitive or relating to subjective judgements (Antcliffe, 2021).

Accuracy of data is particularly important when shared or used as part of automated decision-making, as any impacts from inaccuracy are compounded. For example, a study on children's social care found that automated models missed four out of every five children at risk, and when identifying children at risk, were wrong on six out of ten occasions, meaning that such an inaccurate identification could be added to a child's social care file (What Works for Children's Social Care, 2020). This demonstrates the compelling need for these systems to be built with data protection by design and default,‡ and the need for parents, caregivers and children to be empowered to assert their rights in relation to automated decision-making (Edwards et al., 2021; Redden, 2020; UN OHCHR, 2021).§

Conclusion

To successfully share children's data in their best interests, organisations should carry out a DPIA; take a child-centric, holistic approach; build on existing best practice; and collaborate with other stakeholders. Organisations must ensure effective accountability is in place; minimise the amount of data being processed; be transparent and educate children; ensure the accuracy of data; and create a culture where staff are empowered to safely share data.

Data protection legislation provides a child-centric, proportionate, flexible and risk-based approach to sharing data that supports and empowers organisations to decide for

† Article 5(1)(d) and Article 16 of the UK GDPR require data to be accurate.

‡ Article 25 of the UK GDPR.

§ Article 22 of the UK GDPR provides these rights.

themselves how, what and when to share data. Crucially, it enables an approach that balances the risks of sharing data with the risks of not sharing data, centring a child's best interests in these decisions. The ICO is committed to supporting organisations sharing personal data in children's best interests and highlighting good practice. It recently published additional data-sharing case studies following engagement with Ofsted, and worked with a design company to redesign best interests guidance for organisations (ICO, n.d., e, f).

The ICO's Data Sharing Hub and Children's Code resources house a suite of non-statutory resources for stakeholders including toolkits, case studies, frequently asked questions and guidance. These all demonstrate what 'good' looks like, and organisations are encouraged to use these hubs as the launchpad for any data-sharing initiatives they may want to undertake.

Antcliffe, M. (Host) (2021). Reflections on accessing care records and supporting good recording. Research in Practice podcast, 12 March

BBC News (2021). Schools pause facial recognition lunch plans. 25 October

Butt, E. (2020). *Know economic abuse: 2020 report*. The Co-operative Bank and Refuge

Campbell, N. (2022). Domestic abuse alert scheme extended to 77 more schools in NI. *Belfast Telegraph*, 2 February

Das, G., Cheung, C., Nebeker, C., Bietz, M., & Bloss, C. (2018). Privacy policies for apps targeted toward youth: Descriptive analysis of readability. *JMIR mHealth and uHealth*, 6(1), e3

DCMS (Department for Digital, Culture, Media & Sport). (2021). *Data: A new direction*. 10 September

DfE (Department for Education). (2016). *Information sharing to protect vulnerable children and families: A report from the Centre of Excellence for Information Sharing*. July

DfE. (2018). *Data protection: A toolkit for schools*. July

DfE. (2022). *Complete the school census: Data items 2021 to 2022*. 14 January

Edwards, R., Gillies, V., & Gorin, S. (2021). Data linkage for early intervention in the UK: Parental social license and social divisions. *Data & Policy, 3*, E34. doi:10.1017/dap.2021.34

FCA (Financial Conduct Authority). (no date). Women's economic empowerment. TechSprint 2021

HM Government. (2018). *Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers*. July

ICO (Information Commissioner's Office). (2020a). The benefits of sharing personal data - What can we learn from Open Banking? Blog, 6 January

ICO. (2020b). *Data sharing: A code of practice*

ICO. (2020c). Navigating the data sharing code. In *Data sharing: A code of practice*

ICO. (2020d). Data sharing and children. In *Data sharing: A code of practice*

ICO. (2020e). *Age appropriate design: A code of practice for online services*

ICO. (2020f). Annex D: DPIA template. In Age appropriate design: A code of practice for online services. September

ICO. (2020g). Department for Education (DfE) - *Data protection audit report*. February

ICO. (2020h). Statement on the outcome of the ICO's compulsory audit of the Department for Education. 7 October

ICO. (2020i). Guidance on AI and data protection. 30 July

ICO. (2021a). *Response to DCMS consultation 'Data: A new direction'*. 6 October

ICO. (2021b). Sharing personal data in an emergency - A guide for universities and colleges. Blog, 14 September

ICO. (2021c). *Designing data transparency for children: Insights from the children's code transparency champions open call*. June

ICO. (no date, a). Background to the children's code | About the ICO

ICO. (no date, b). Research and reports | About the ICO

ICO. (no date, c). London School of Economics and Political Sciences (LSE) | Grants programme

ICO. (no date, d). Examples of processing 'likely to result in high risk' | Guide to the GDPR

ICO. (no date, e). Best interests of the child self-assessment | Children's Code Hub

ICO. (no date, f). Case studies and examples | Data Sharing Information Hub

ICO. (no date, g). Accountability and governance | Guide to the GDPR

ICO. (no date, h). *Findings from the ICO's consensual audits of 11 multi academy trusts, September 2018 to October 2019*

Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society, 19*(5), 780-794

Munro, E. (2011). *The Munro review of child protection: Final report – A child-centred system*. May. Department for Education

National Infrastructure Commission. (2017). *Data for the public good*

NSPCC. (2021). Protecting children from domestic abuse

Ofcom. (2021). *Online nation, 2021 report*. 9 June

Redden, J. (2020). Predictive analytics and child welfare: Toward data justice. *Canadian Journal of Communication, 45*, 101-111

Ritschel, C. (2019). Justin Bieber acknowledges using racial slur as a teen while asking fans to 'stand against racism'. *Independent*, 4 December

UN OHCHR (United Office of the High Commissioner for Human Rights). (1989). *Convention on the Rights of the Child*. 20 November

UN OHCHR. (2021). *The right to privacy in the digital age: Report (2021)*

Wang, G., Zhao, J., & Shadbolt, N. (2019). Are children fully aware of online privacy risks and how can we improve their coping ability? *ArXiv*. abs/1902.02635

Watson, P. J. (2021). England cricketer gets international ban for edgy tweets he posted when he was a teenager. *Summit News*, 7 June

What Works for Children's Social Care. (2020). *Machine learning in children's services: Summary report*. September

Women's Aid. (2022). *The domestic abuse report 2022: The annual audit*

Women's Aid. (no date). What is domestic abuse? Impact on children and young people

Legislation

Domestic Abuse Information-sharing with Schools etc. Regulations (Northern Ireland) 2022 (NI) (UK)

1 http://waspi.org/information-sharing-protocols

2 https://ico.org.uk/for-organisations/posters-stickers-and-e-learning/school-resources