GDPR compliant school social media use — recommended guidance

Based on her own research into existing guidance on school social media use, Dr Claire Bessant, Associate Professor at Northumbria Law School, outlines key issues for schools considering posting children's images on social media, interpreting guidance from the DPC and the UK's ICO

Schools across the globe are increasingly using social media to engage with communities, circulate information and celebrate staff and pupils' achievements. In Ireland, whilst the Data Protection Commission's ('DPC') blogpost on 'Taking photos at school events' refers to children's images being shared on school websites, it does not mention school social media. In the UK, the practice is recognized by both the Department of Education ('DfE') and the Welsh government, however, neither body has provided detailed guidance explaining how schools can ensure social media use complies with the GDPR. The brief, undated guidance from the UK Information Commissioner's Office ('ICO') referenced by the DfE ('Taking photographs: Data protection advice for schools') does not discuss social media use, and neither does the ICO's general GDPR or Children and the UK GDPR guidance.

Many education authorities are addressing this advice gap by providing detailed guidance on school use of images and template consent forms. This article outlines concerns raised by some of these education authority documents, and offers recommendations for schools using social media, suggesting how they might satisfy GDPR requirements and properly respect children's rights.

Regulator Guidance

Both the DPC's 'Fundamentals for a child-oriented approach to data processing' ('the Fundamentals') and the ICO's 'Children and the UK GDPR' guidance detail key principles governing the processing of children's data. These documents remind controllers that children are afforded rights not only by the GDPR but also by the United Nations Convention on the Rights of the Child ('UNCRC').

Whilst the UNCRC imposes obligations primarily upon states, UNICEF, through its Children's Rights and Business Principles, calls upon all organisations to, 'meet their responsibility to respect children's rights and commit to supporting the human rights of children', 'ensure the protection and safety of children in all business activities', and 'use marketing and advertising that respect and support children's rights (Principles 1, 4 and 6).

Article 16 UNCRC affords children a right to privacy. Article 3 UNCRC stipulates that in all actions concerning children, the best interests of the child must be a primary consideration. The 'core message' of the Fundamentals "is that the best interests of the child must always be the primary consideration in all decisions relating to the processing of their personal data." These views mirror the 2009 Opinion of the European Data Protection Board's predecessor, the Article 29 Working Party, that the best interests principle 'must be respected by all entities, public or private, which make decisions relating to children'. The ICO confirms that although the UK GDPR does not specifically mention children's best interests, it expects controllers to consider Article 3 before processing children's personal data.

The Fundamentals stress the importance of Data Protection Impact Assessments ('DPIAs') and data protection by design and default where children are concerned. The ICO also suggests that controllers design processing with children in mind, using a data protection by design and by default approach. The regulator further advises in line with Recital 38 of the UK GDPR that controllers processing children's personal data consider from the outset how special protection is afforded to children's data, suggesting a DPIA is used to assess and mitigate data protection risks to the child.

The ICO prompts controllers to consider Article 12 UNCRC, recalling that 'every child has the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously.' The Article 12 right to express a view is afforded to every child capable of expressing a view. The weight given to a child's views will depend upon the child's age and maturity, with greater weight given to the mature child's views. The ICO's guidance for England and Wales reflects this 'developing capacity'

approach, advising controllers to consider the child's competence (their capacity to understand the implications of processing). Children with such capacity are competent to give their own consent unless they are acting contrary to their own best interests.

In Ireland, Fundamental 7 explicitly requires controllers to 'let children have their say'; it reminds controllers that a child may exercise their rights at any time, provided they have capacity and it is in their best interests. DPC guidance again emphasises the need to consider the child's age and maturity. No age limit applies to children in England, Wales or Ireland outside the context of ISS (information society service) consent. In Scotland, however, a child is assumed to have capacity to consent to processing if they have a general understanding of what it means to give consent, it being presumed that children aged 12 and above are of sufficient age and maturity to have such understanding (as per section 208 of the UK Data Protection Act 2018/ 'DPA 2018').

"One option suggested by the DPC where parents do not want their children to be photographed at an event is for schools to provide children with coloured stickers to signify whether or not they can be photographed."

Children are, of course, only able to comment upon data processing if told how and why their data are being processed. The ICO emphasises that transparency is key; that controllers should provide clear, age-appropriate privacy notices to children/parents, explaining how children's data will be used; the risks inherent in processing; and how the controller will safeguard against those risks. Fundamental 5 confirms that children are entitled to receive information about processing irrespective of the legal basis relied upon, and even where consent is provided by their parent. Fundamental 6 emphasises the importance of 'child-oriented transparency'. As discussed further below, UK education authority documentation on children's image use does not routinely provide such transparency for children or parents.

Primary research into education authority guidance

In December 2021, Freedom of Information Act 2000/Freedom of Information Act (Scotland) Act 2002 requests were sent to all 205 education authorities in England, Scotland and Wales asking: 'Please confirm whether the authority has developed policies or guidance on school use of children's images, whether on school websites, on social media pages or any other media; and if such policies/guidance exist a copy of the policy or guidance and any related templates or example documentation including consent forms and privacy notices is requested.'

15 authorities failed to respond; 125 authorities stated that they did not hold the requested information or that disclosure would prejudice the authority's commercial interests; and 65 authorities (29 English, 9 Welsh and 27 Scottish) disclosed substantive information about their advice to schools, including detailed guidance, photography/ image use policies, template privacy notices and consent forms.

All 65 authorities advised schools to obtain consent before sharing photographs which might identify a child. This reflects DfE advice that schools should obtain consent prior to sharing children's photographs online. Most template consent forms, however, offered no more than a list of tick boxes. Few documents disclosed would effectively inform children/parents or assist them in determining whether social media use would be in a child's best interests.

Practical guidance for schools

Where consent is relied upon as the lawful basis for processing, the data subject gives 'consent to the processing of his or her personal data for one or more specific purposes' (Article 6(1)(a) of the UK/EU GDPR). Consent here means 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (Article 4(11)).

Using these consent provisions as a lens through which to explore authorities' guidance, below are suggestions for how schools can satisfy the GDPR's transparency requirements and secure valid consent.

'Consent is 'freely given' where data subjects have a genuine choice'

As the ICO explains, 'people must be able to refuse consent without detriment.' One authority commented 'if we do not have permission to use the image of your child, it may result in your child not being able to take full part in some school events'. This contravenes Article 4(11) and raises questions about children's best interests being treated as a primary consideration.

Recommendation: If the sharing of children's images on social media could place a child at risk of harm, or where a child/parent does not wish the child's image to be shared on social media, the child/parent should be able to refuse consent without this impacting upon the child's ability to engage with educational activities. One option suggested by the DPC where parents do not want their children to be photographed at an event is for schools to provide children with coloured stickers to signify whether or not they can be photographed.

(Continued on page 6)

(Continued from page 5)

'Consent must be specific'

A consent request must cover all different purposes and types of processing for which controllers seek consent. The DfE's data protection guidance includes a template consent form asking parents to consent to the school taking photographs 'to use on [for example, the school website, school prospectus, or social media — have a separate box for each]'. Where schools seek blanket consent for all social media, parents cannot gauge where children's images will appear, and how a child's privacy may be impacted.

Some authorities' guidance raised issues regarding the use of blanket consent. 19 authorities sought blanket consent for all online use. 14 authorities outlined examples of social media platforms that might be used then sought consent for all social media use, offering no option to consent/refuse consent for specific platforms. Only five authorities suggested school consent forms detail each specific social media platform used and seek consent in relation to each different platform.

Recommendation: Schools should use a more granular approach, as this recognises that different platforms may pose different privacy risks, and permits children/parents to select/deselect specific platforms where images may be shared.

The ICO also advises that consent requests should be prominent, concise, and separate from other terms and conditions. Some authorities included requests for consent to image use within school handbooks, school acceptable usage policy or within general permission forms issued upon school enrolment. The recommended approach used by most authorities is to include consent requests in separate photographic policies/consent forms.

'Consent must be informed'

Articles 5(1)(a), 12 and 13 of the UK GDPR require schools to clearly explain to children/parents what they are consenting to in a way they can easily understand. Information should be provided about what is being shared, the platforms where information will be shared, the potential recipients of children's personal data, and the benefits and risks of social media dissemination. This way, children/parents can weigh up the pros and cons of online publication.

24 authorities indicated in their template consent forms that children's photographs, videos and images would be shared online, but failed to clarify whether images may be accompanied by further information, such as a child's name, thus preventing parents/children from fully understanding how social media use might threaten children's privacy. Only 25 of the 65 authorities who disclosed their guidance (38%) suggested schools inform children/parents why schools are using social media. Even fewer authorities (7%) suggested schools provide information about the risks of sharing children's images on social media, and the information provided was limited (for example, 'images used on the internet/websites may be viewed by any person with internet access worldwide' and 'the school cannot control who will view the images or the countries in which the images may be accessible').

Not a single authority suggested that schools explain how online publication may threaten children's privacy and welfare. As the Welsh government reminded schools earlier this year, 'images can be collected by third parties that schools may not be able to see, identify or stop.' All images published publicly online can be copied, downloaded, screenshotted, shared, adapted and used inappropriately, and in ways that were not consented to. This can have long term implications for children and their self-esteem. Children's images shared on social media are being harvested, manipulated and misused by companies and by paedophiles. The sharing of children's images on social media also contributes to a child's digital shadow, the data associated with children that we cannot see that is used to make assumptions and predictions about individuals and groups of children.

Only 20 authorities mentioned using 'safeguards' to protect children's privacy and welfare, such as never publishing an image of a child in revealing attire and not providing a child's full name alongside their image. Whilst the risk of identification is lower if a child's name is not provided, children's names are not the only means of identifying a child. The Welsh government cautions against sharing images alongside any information which may be used to identify a child, including personal details and location tags. Since a pupil's location can be inferred from their schools' social media posts, by posting children's images online, even without a name, schools can unintentionally compromise children's privacy and expose them to risks of identify fraud, harassment, stalking and grooming.

Consideration of all potential risks is key to compliance with the Article 3 UNCRC best interest principle, which obliges schools to assess and weigh the benefits of social media use with risks posed to children's privacy, safety and wellbeing by such social media use. Article 3 requires schools to go beyond UK GDPR compliance, to consider what is ethical and acceptable to parents and children, particularly bearing in mind that the long-term implications of sharing children's images on social media are unknown.

Recommendations: Privacy notices or consent forms should be used to provide parents/children with age-appropriate information about the context in which photographs are going to be taken (for example the types of school events and activities where photography will take place), the specific data likely to be shared, the platforms used, and the risks posed by school social media, to enable them to determine whether disclosure is in a child's interests.

Parents/children should be told how long images will be kept for, and that they have a right to withdraw consent to the future use of such images at any time. Schools should be mindful of the information given to parents/children in privacy notices and consent forms which cover the full

school year; if the nature and context of photography fundamentally changes, for example because photographs are going to be taken at an event where parents might not expect them to be taken or because photographs are going to be posted somewhere different and unexpected, schools should seek additional consent.

Schools should use a DPIA to identify and address risks posed by social media use. To minimise threats to children's privacy and in accordance with the ICO's advice to take a data protection by design and default approach, schools could take photographs showing children facing away from the camera. They could take photographs at a distance or share images only of children in large groups, rendering them unidentifiable by either third parties and facial recognition technology.

The Welsh government also suggests that before posting any image online, schools consider who will be able to see the image and how they could use it; whether there is a better way to share the image than on a public site; and whether posting the image could expose a child or young person to any risks or make them vulnerable. Where a school wishes to build community, it could make school social media pages private, minimising the chances that individuals unconnected with the school will find pupils' photographs. Where schools wish to celebrate children's achievements with the wider community, pupils' first names could be used without images.

'Consent requires an unambiguous indication of the data subject's wishes by a statement or clear affirmative action'

Although three authorities produced multiple guidance documents offering contradictory advice about use of opt-in or opt-out consent, the remaining 62 authorities advised schools to obtain opt-in consent, reflecting the requirement for clear affirmative action.

Notwithstanding the ICO's reminder that Article 12 UNCRC affords children a right to express their views and to have their views taken seriously, many child data subjects are, however, never formally told or consulted about school social media use. Only five authorities provided child-friendly/child-focused privacy notices; only one notice suggested children's photographs might be used on social media. The DfE template referred to above affords no opportunity for children to provide consent, seeking parental signature only. Similarly, 32 authorities (49%) advised that schools must always obtain consent from parents, with three further authorities advising schools obtain parental consent for all pupils under eighteen. The remaining authorities recognised, in line with DPA 2018 and ICO guidance, that children develop capacity to consent. Nonetheless many authorities misunderstood the legal position, with some Scottish authorities failing to recognise that children aged 12 and above are presumed to have capacity and the suggested age of consent varying from 8-18.

Finally, 14 authorities advised that consent, once obtained, would last for the duration of the child's time at school, unless withdrawn by the parent. In those authority areas, children cannot, therefore, provide consent when they develop capacity.

Recommendations: Schools should seek consent annually/bi-annually to ensure the developing child can contribute their views. Parental consent forms should encourage parents to discuss with their children how schools use children's images.

The following approach to seeking consent, used by two authorities, is recommended: parental consent should be obtained for younger children (for example, primary school children/under 12s); slightly older children (for example children in the early years of secondary school, or who are aged12-15 years-old are likely to have capacity to consent, and as a minimum should be asked to sign forms alongside their parents. pupils aged 16 and above will, ordinarily, be able to provide sole consent. Even where parental consent is sought, schools should provide children with age-appropriate information about how schools use their images and encourage parents to seek children's views Where children object to their photographs being shared on social media their views should be listened to.

Dr Claire Bessant
Northumbria University, School of Law
Claire.bessant@northumbria.ac.uk