

07 September 2022

New South Wales Department of Education

Cc: Vally Grego, Principal, Moorebank High School
Hon Sarah Mitchell MLC, NSW Minister for Education and Early Learning
Samantha Gavel, NSW Privacy Commissioner

Re: Privacy and digital security concerns regarding Moorebank High School scanning children's fingerprints to access toilets

Dear Secretary,

Digital Rights Watch is an Australian civil society organisation advocating for the protection of human rights in the digital age. We write to express our concern regarding the collection and use of biometric information by Moorebank High School in New South Wales (NSW), and to request additional information regarding the internal risk assessment process regarding the use of biometric surveillance technology on children.

We do so in the spirit of seeking to ensure that the rights of children in NSW are upheld and respected, and would welcome the opportunity to discuss this matter with you further. Below we have outlined our key concerns, and included several questions for further clarification.

It is our view that the collection and use of children's biometric information for the purpose of protecting school property from vandalism is an unreasonable and disproportionate invasion of privacy. **We urge Moorebank High School to cease the use of this technology, and that the NSW Department of Education commit to preventing future use of biometric surveillance technology in other schools.**

Our concerns are as follows:

1. Collection and use of children's biometric information sets a dangerous precedent for other schools, and contributes to the normalisation of surveillance.

The implementation of such a system teaches children from a young age to readily accept and expect invasion of their privacy. This is a concerning normalisation of surveillance, and strips children of agency over their bodies and the privacy of their personal information. In an age of ubiquitous data harvesting facilitated by digital technology, we ought to be teaching children to think critically about their privacy and digital security, and equipping them with the skills to protect their personal information, not forcing them to surrender it.

While we understand the system has been deemed 'optional', its existence places unreasonable pressure upon children and their parents to comply—evidenced by the majority of the school's 1000

students having already registered their fingerprints to use the bathroom in school hours.¹ Should other schools see the use of this technology and also decide to implement it for the same or similar purposes, there is a significant risk that requiring children to scan their fingerprints will become the norm in NSW.

2. The collection of children’s biometric information creates additional and unnecessary digital security risk, ultimately undermining the safety of Moorebank students.

Simply by collecting and storing biometric information, Moorebank High School (and any third party technical supplier), is significantly increasing the risk and possible consequence of a security incident, such as a data breach. Should the data be leaked, hacked or otherwise accessed by unauthorised means, Moorebank students are at serious risk of negative consequences, including identity fraud.

The nature of biometric information is extremely sensitive. This is because it is intrinsically linked to our physical bodies, and cannot readily be changed. Once the security of this information is compromised, it is extremely difficult to mitigate the flow-on harms.

Further, we note that media reports have quoted school representatives saying that the Poliflex Kiosks do not store a copy of students’ fingerprints, but instead captures an “alphanumeric representation” of the fingerprint, which is stored off-site. This represents a fundamental misunderstanding of how biometric templates work in practice, and we wish to emphasise that the collection and storage of a unique representation of a fingerprint is *no less invasive* than storage of the fingerprint itself.

3. The collection and use of biometric information may not be compliant with privacy law

Moorebank High School and the NSW Department of Education are regulated by the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA), which requires that certain criteria be fulfilled before the school can lawfully collect fingerprints of children.

Notably, the collection of personal information must be “reasonably necessary” for the designated purpose, which media reporting indicates is to reduce instances of vandalism of school toilets. This requires Moorebank and the Department to assess whether the collection of biometric information is a *proportionate* response to the issue of vandalism. It is our view that collecting children’s biometric information is a significant overreach, and that there are less privacy-invasive alternatives. Biometric surveillance is a disproportionately intrusive approach.

The PPIPA also requires that the information collected is relevant to its purpose, not excessive, accurate and complete, and that the collection of the information does not intrude to an unreasonable extent on the personal affairs of individual students. Moorebank and the Department must also take steps to ensure that students, parents and guardians are notified before any collection takes place, as well as other relevant details. In addition to this, once personal information is held by a school, or a technology vendor on the school’s behalf, it must meet additional obligations regarding the security, access and accuracy of that data, as well as limitations on how that information can be used or disclosed.

¹ ‘Sydney high school uses fingerprint technology to stop vandalism in toilets’, *The Guardian*, 6 September 2022. Available at: <https://www.abc.net.au/news/2022-09-06/moorebank-high-school-fingerprints-students-going-to-toilet/101410544>

We are concerned that scanning children's fingerprints to access the toilet may not be compliant with the PPIPA, and request additional information, including a Privacy Impact Assessment and clarification as to whether the Department conducted an evaluation of the system purchased by the school prior to implementation.

We would appreciate additional clarifying information regarding the risk assessment and decision making process. Our questions are as follows:

1. Reporting by 9News indicated that Moorebank High School implemented the use of Posiflex Kiosks Biometrics upon suggestion from the NSW Department of Education.² Can you please confirm if this is the case, or if the school independently decided to implement the use of this technology?
2. If the above is true, has the NSW Department of Education recommended the use of biometric surveillance technology, including but not limited to facial recognition systems, exam proctoring software, or fingerprint-based facility access, or similar technology, to any other schools?
3. Was a Privacy Impact Assessment (PIA) completed by the Department, or by Moorebank High School prior to commencing its use, and if so, can you please provide a copy of the PIA to us so we can understand how the privacy and digital security risks were identified and mitigated.
4. How many people in the Department are dedicated to privacy compliance, completing PIAs, or giving proactive privacy advice to schools in NSW (as opposed to just responding to complaints)?

Thank you for your time. We look forward to your response and would welcome the opportunity to discuss this matter further with you.

Sincerely,

Samantha Floreani
Digital Rights Watch

² 'Sydney high school uses controversial technology to stop vandalism in toilets', 9News, 6 September 2022. Available at:

<https://www.9news.com.au/national/moorebank-high-school-introduces-fingerprint-scanning-technology-to-stop-graffiti-and-anti-social-behaviour/e9fd3dc4-3420-4a58-a04d-e40f88c2f91d?ocid=Social-9NewsS>