AICYBERLEX NEXUS

Journal of Artificial Intelligence, Cyber & Contemporary Law

Volume I · **Issue I** · **Jul–Sep 2026** · Article 2
ISSN: Applied for (National ISSN Centre, NIScPR, India) · e-ISSN: TBA
Peer-reviewed · Open Access · https://aicyberlexnexus.com

ARTICLE 2

Universities as Data Fiduciaries: Reading the Digital Personal Data Protection Act, 2023 in the Campus Context

Pawan SS

LL.M. (Digital Technology, Policy & Governance), National Law University Delhi

ABSTRACT

A university holds more personal data about a young person than almost any other institution does. It knows the applicant's marks, caste category, family income, medical certificates, disciplinary record, hostel address, face on camera and every grade ever awarded. The Digital Personal Data Protection Act, 2023 treats an institution that decides why and how such data is used as a "data fiduciary", but it says nothing specific about universities. This paper reads the Act's general duties against the day-to-day life of an Indian campus. It argues that universities are fiduciaries in the fullest sense, that several ordinary campus practices sit uneasily with the Act, and that the hardest cases are those involving minors, examinations, surveillance and research. It closes with practical recommendations that a registrar's office could act on without waiting for new law.

KEYWORDS: data fiduciary; DPDP Act; universities; students' data; consent; children's data

1. Introduction

Ask a final-year student how many times her data was collected before she reached the convocation hall, and she will probably not remember. An application form, an entrance test registration, a fee receipt, a library card, a hostel allotment, a biometric attendance system, an online proctoring session, a placement portal. Each step asks for something, and each answer is stored somewhere. For years the legal framework around this was thin. Section 43A of the Information Technology Act, 2000 and the 2011 rules on sensitive personal data were the main tools, and few universities treated them as binding on their own conduct. The Supreme Court's recognition of privacy as a fundamental right in Puttaswamy changed the constitutional picture, but day-to-day compliance on campuses stayed patchy.[1] The Digital Personal Data Protection Act, 2023 (the DPDP Act) is meant to change that. It was followed by the Digital Personal Data Protection Rules, notified in November 2025 with a phased timetable for different obligations.[2] The Act is general. It does not carve out a chapter for education. This paper therefore asks what the general rules mean when applied to a university: whom the university owes duties to, what those duties are, and where the Act's wording does not fit campus reality. The paper has six parts. Part 2 explains why a university is a data fiduciary. Part 3 sets out the main duties. Part 4 takes up some hard cases. Part 5 identifies gaps and gives recommendations, and Part 6 concludes.

1

2. Why a university is a data fiduciary

Section 2(i) of the Act defines a data fiduciary as any person who, alone or together with others, determines the purpose and means of processing personal data. A "person" includes a company, a firm, an association and "every artificial juridical person".[3] A university, whether central, state, private or deemed, fits comfortably within that wording. It decides what to collect from students, staff and applicants, and it decides what to do with it. Two points are worth stressing. First, the status does not depend on ownership. A state university and a private one are both fiduciaries. The difference lies in which legal grounds for processing are available to them, as discussed below. Second, a university often shares its fiduciary role. Where it uses a learning-management platform, an online proctoring vendor or a cloud host, those vendors are data processors acting on its behalf. The Act leaves the responsibility with the fiduciary even if the processor is the one who loses the data.[4] A registrar cannot escape by saying "the vendor did it". The word "fiduciary" is not decoration. It signals a relationship of trust in which one side has the power and the other has little choice. A student cannot realistically say no to an enrolment form. The Act's design leans on that unequal relationship, which is why the duties it places on universities are heavier than the language of "consent" alone might suggest.

3. The main duties under the Act

3.1 Notice and consent Under sections 5 and 6, processing generally needs consent that is free, specific, informed, unconditional and unambiguous, and the request must come with a notice describing the data, the purpose and the means of withdrawing consent. For a university this means the admission form can no longer carry a vague line such as "I agree to all rules of the university, as amended from time to time". Each purpose, from admission processing to alumni fundraising, needs to be described in plain terms. 3.2 Legitimate uses Section 7 lists situations where consent is not needed. Two matter for universities. Where an individual voluntarily gives data for a stated purpose and does not object, that use may proceed (section 7(a)). And the State and its instrumentalities may process data to give subsidies, benefits and services, or to perform functions under law (section 7(b) and (c)). A public university distributing a scholarship can use the second ground. A private university running a placement drive probably cannot, and must rely on consent or on the voluntary-provision ground. Section 7(i), covering employment, helps with staff records. 3.3 Accuracy, safeguards and breach Section 8 collects the central duties. The fiduciary must keep personal data accurate where it is used for decisions or disclosed (8(3)), apply reasonable security safeguards (8(5)), tell both the Data Protection Board and each affected person when a breach occurs (8(6)), and erase data once the purpose is served unless the law requires retention (8(7)). It must also publish contact

2

details of someone who can answer questions (8(9)). The financial stakes are real. The Schedule to the Act sets a penalty of up to Rs 250 crore for failure to take reasonable security safeguards, and up to Rs 200 crore for failure to notify a breach or to meet the children's data obligations.[5] A university that treats its student database as an afterthought is carrying a large unpriced risk. 3.4 Rights of students Students, as data principals, have rights to access a summary of their data and the identities of those it has been shared with (section 11), to seek correction and erasure (section 12), to have grievances addressed (section 13), and to nominate someone to exercise rights

on their behalf (section 14). Universities will need an internal process, with named people and fixed timelines, to receive and answer such requests.

4. Hard cases on campus

4.1 Students under eighteen Many first-year students, especially in five-year integrated programmes, enter university at seventeen. Under section 9 the data of anyone below eighteen can be processed only with verifiable consent of a parent or lawful guardian, and the fiduciary must not track or monitor the behaviour of children or target advertising at them. The Rules offer limited exemptions for educational institutions to monitor behaviour where it is needed for educational activities or safety.[2] How far these exemptions stretch is not obvious. A university will want to read them narrowly and document its reasoning. 4.2 Examinations and results Exam records create a tension between transparency and privacy. In CBSE v Aditya Bandopadhyay the Supreme Court accepted that examinees are entitled to inspect their own evaluated answer scripts under the Right to Information Act.[6] The DPDP Act amends section 8(1)(j) of the RTI Act, which deals with personal information, and the effect of that change on requests for other students' marks and rank lists is likely to be argued in courts. For now, universities should separate what a student may see about herself from what may be published about the whole cohort. 4.3 Surveillance and proctoring Cameras in corridors, facial recognition at library gates and AI-assisted online proctoring all collect biometric or video data at scale. Because the Act does not create a separate class of "sensitive" data, the reasonable safeguards test of section 8(5) and the purpose limitation principle do most of the work. A university that records every lecture hall for security should ask whether the footage is kept longer than needed and who can view it. The answer in many places today is: indefinitely, and nearly anyone. 4.4 Placements and sharing with employers Handing CVs, grades and contact details to recruiters is routine. It is also a disclosure of personal data to third parties. Students should know what is being shared and with whom, and

should be able to decline particular recruiters without fear of being dropped from the process. 4.5 Research data Section 17(2)(b) exempts processing for research and statistical purposes where the data is not used to make decisions about a specific person and is handled in line with prescribed standards. This is helpful for academic studies, but it does not cover the university's own administrative analytics. A dashboard that flags students at risk of dropping out is making a decision about individuals, and the research exemption will not shelter it.

5. Gaps and recommendations

Three gaps stand out. The first is a mismatch of capacity. Many universities, particularly state institutions, have small IT teams and no one trained in data protection. The Act assumes a level of internal governance that does not yet exist. The second is uncertainty about the position of public universities. They are treated as "State" for many constitutional purposes, which brings both wider grounds for processing and the burden of the exemptions under section 17, and the resulting picture is unclear. The third is the thin guidance on children. A rule that protects minors in principle but leaves a campus unsure whether biometric attendance is lawful is of limited use. Against that background the following steps are realistic. A university should first map the data it holds: what is collected, from whom, for what purpose, where it is stored and who can reach it. Without this inventory, every other step is guesswork. It should then replace blanket admission-form consents with purpose-specific notices written in plain language, with English and regional-language versions where needed. It should appoint a named officer to handle

data principals' requests and publish contact details as section 8(9) requires, and it should set a fixed timeline for responses. Retention schedules should be adopted so that records are deleted or archived once their purpose ends. Admission data of unsuccessful applicants is an obvious first candidate. Vendor contracts should be reviewed so that processors are bound to security standards, breach reporting and deletion on exit. Finally, an incident plan should be written down before the first incident, including who informs the Board and the students, and how quickly.

6. Conclusion

A university is a data fiduciary because it decides what happens to the personal information of thousands of people who have little say in the matter. The DPDP Act gives that status teeth: notice, consent, security, breach reporting and deletion, backed by large penalties. The Act's general language leaves campus-specific questions open, especially on minors, surveillance and the position of public universities. Until guidance catches up, universities are best served by treating the Act as a prompt for housekeeping they should have done already. A student who

4

hands over her marks, her face and her family's income is trusting the institution. The law now says that trust has a price if it is broken.

References [1] Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1. [2] Digital Personal Data Protection Rules, 2025 (notified November 2025; phased commencement). Readers should check the current text of the Rules and their schedules before relying on any particular exemption. [3] Digital Personal Data Protection Act 2023, s 2(i), s 2(s). [4] Digital Personal Data Protection Act 2023, s 8(1)-(2). [5] Digital Personal Data Protection Act 2023, ss 5-9, 11-14, 17, and the Schedule. [6] Central Board of Secondary Education v Aditya Bandopadhyay (2011) 8 SCC 497.

5

Cite as: Pawan SS, “Universities as Data Fiduciaries: Reading the Digital Personal Data Protection Act, 2023 in the Campus Context”, *AICyberLex Nexus*, Vol. I, Issue I, Jul–Sep 2026, Article 2. Available at https://aicyberlexnexus.com
© 2026 AICyberLex Nexus. Open access under the terms stated on the journal website.