Bentley® Education

Data rights and permissions considerations

This framework provides an organized overview of key actions for managing data in a campus digital twin, including ownership, licensing, compliance, and ethical use. It supports regulatory adherence, transparency, and trust among stakeholders while ensuring the digital twin operates effectively. Use this table as a practical reference for ongoing data management throughout the project life cycle.

Category	Key actions	Notes
Data ownership	Identify ownership of campus-related data (e.g., university, third-party contractors, students, staff).	Ownership may vary by data type, such as IoT sensor data, building information, or activities.
	Clarify ownership for different data categories.	Clearly defined ownership simplifies permissions and compliance.
Data licensing	Define licenses for campus data (e.g., open data for research, restricted use for internal purposes).	Use consistent licensing terms to align with institutional policies.
	Set terms for external access by researchers, students, or partners.	Ensure that licensing reflects data sensitivity and intended use.
Data access and permissions	Establish access levels for stakeholders (e.g., facilities managers, students, researchers).	Access should align with roles and responsibilities.
	Protect sensitive data, such as students' personal information or security details.	Use robust security protocols to prevent unauthorized access.

Data sharing agreements	Develop agreements for sharing data with external parties (e.g., government, research institutions).	Agreements should detail terms of use, access, and restrictions.
	Ensure compliance with laws like GDPR when sharing with third parties.	Regularly review agreements to ensure they remain current and compliant.
Compliance with data regulations	Ensure data collection complies with regulations like GDPR.	This includes obtaining consent for collecting personal or sensitive data.
	Train staff on compliance best practices and monitor adherence.	Ongoing reviews ensure alignment with updated regulations.
Data anonymization	Anonymize individual-related data (e.g., campus traffic patterns, student movement) before analysis or sharing.	Robust anonymization protects privacy and reduces risks.
	Regularly update anonymization techniques to adapt to emerging threats.	
Intellectual property (IP)	Clarify IP ownership for digital twin data (e.g., university vs. software providers).	Collaboration agreements should explicitly define IP rights.
	Address IP ownership for research outcomes associated with the digital twin.	
Ethical considerations	Communicate transparently how campus data will be used (e.g., monitoring, service improvement).	Regular communication builds trust among stakeholders.
	Monitor for misuse (e.g., intrusive surveillance) and enforce ethical standards.	

Data retention and deletion	Set policies for retaining different types of campus data (e.g., personal vs. operational data).	Include clear guidelines on data life cycle management.
	Establish protocols for securely deleting personal data when no longer needed.	Ensure secure and irreversible deletion processes.