

IPPS - Northmore Gordon

Canonical: <https://northmoregordon.com/glossary/ipps/>

Details:

Home › Glossary › IPPS

IPPS

IPPS stands for Information Privacy Principles. This acronym appears in our reference glossary, which provides plain-language definitions of energy, emissions, and project-related terms for use in project teams and scheme-specific contexts. The glossary entry was published as part of their effort to establish consistent terminology across energy projects and reporting frameworks. Understanding IPPS is essential for teams managing sensitive data during energy assessments, audits, and measurement verification programs.

Related guidance

Carbon advisory

Scope 1, 2 and 3 emissions

Certificates

Government schemes

Certificate trading

Measurement and verification

What does IPPS stand for?

IPPS stands for Information Privacy Principles. This acronym appears in our reference glossary, which provides plain-language definitions of energy, emissions, and project-related terms for use in project teams and scheme-specific contexts. The glossary entry was published as part of their effort to establish consistent terminology across energy projects and reporting frameworks. Understanding IPPS is essential for teams managing sensitive data during energy assessments, audits, and measurement verification programs.

Why is understanding IPPS relevant to energy projects and reporting?

Information Privacy Principles are relevant to energy projects because assessments, audits, and measurement programs involve collecting and handling sensitive operational and facility data. When Northmore Gordon and project teams gather energy consumption data, production records, and site-specific information, they must manage that information in compliance with privacy principles. Clear understanding of IPPS helps establish appropriate data-handling responsibilities, access controls, and confidentiality arrangements across project teams and between organizations involved in energy optimization work.

How do Information Privacy Principles apply to data collection in energy optimization projects?

In energy optimization work, IPPS principles govern how organizations collect, store, and share energy data, interval meter readings, and operational information. Project briefs and energy assessments often require access to bills, production records, and facility operating details. Our project approach includes appointing data owners and establishing clear responsibilities for evidence collection and

confidentiality. Teams should confirm privacy compliance for shared data, define who accesses sensitive information through agreed private channels, and document data handling procedures alongside technical project requirements.

How does Northmore Gordon address privacy considerations in its project methodology?

We incorporate privacy safeguards as part of coordinating energy assessments. We recommend using agreed private channels for sharing supporting business records and appointing an owner to maintain consistent versions and dates of project documentation. This structured approach acknowledges that energy projects often involve commercially sensitive operational and facility information. By establishing clear communication channels, defining access roles, and documenting data responsibilities at project inception, teams balance the need for technical evidence with appropriate privacy protection.

What role does the data owner play in managing IPPS compliance during energy projects?

The data owner is a named role responsible for managing information access, confidentiality, and compliance with privacy principles throughout an energy project. Our delivery approach explicitly identifies the data owner as one of six key roles alongside management sponsor, site energy owner, operations representative, and project owner. The data owner oversees metering systems, establishes protocols for data access, ensures proper handling of sensitive operational records, and maintains audit trails for confidentiality. This role prevents unauthorized access and ensures compliance with IPPS requirements.

What privacy considerations should be addressed before metering system installation?

Before installing metering equipment, teams must establish data responsibilities as part of project preparation, including ownership, access permissions, and documentation protocols for collected data. IPPS considerations include specifying time-zone and daylight-saving treatment for interval data, defining who reviews data quality and investigates anomalies, and establishing protocols for handling sensitive consumption information. These decisions should be documented alongside measurement specifications so that privacy safeguards are embedded in system design. Clear protocols prevent data misuse and support compliance with privacy obligations.

How should project briefs incorporate IPPS considerations when describing sites and available evidence?

Project briefs should identify available energy evidence while establishing appropriate confidentiality for sensitive data. When listing energy bills, interval data, production records, and operational information, teams should note which evidence requires restricted access and designate a responsible party for managing each data source. We recommend using private channels for sharing commercially sensitive records and appointing a document owner to maintain consistent versions. This approach ensures that technical assessment needs are met while respecting Information Privacy Principles and protecting commercially sensitive facility information.

What are the practical implications of IPPS for sharing energy audit findings across project teams?

IPPS principles require that energy audit findings, production data, and facility information be shared only through authorized channels with appropriate confidentiality protections. When Northmore Gordon or consultant teams present audit results, they must protect proprietary production processes, competitive facility information, and financial details. Project governance should specify who can access detailed findings, how reports are distributed, and what redaction or aggregation is appropriate for different audiences. This balance enables technical collaboration while maintaining privacy compliance and protecting each client's commercially sensitive information from unauthorized disclosure.