Open Data, Privacy and Cyber Security Policy

Urban 360 was spun out of the University of Manchester with the recognition that academic rigor, provenance and accountability in data and software we provide is key to developing a path to sustainable services. Driven by our customer needs, we are committed to the FAIR Guiding Principles for scientific data management and stewardship to improve the **F**indability, **A**ccessibility, **I**nteroperability, and **R**euse of digital assets. This enables us to provide digital services and tools that enable our customers to derive sustainable insights into data and services we provide. We also adhere to the highest standards of data protection and privacy as set out in the 2018 Data Protection Act and the requirements of UK GDPR, to protect the data of clients and all others with whom we interact. We are also committed to maintaining the highest possible level of cyber security across all hardware and software that we use.

Aims

We are committed to embedding open research principles in our business model, across our digital assets. This includes:

- Analytical software
- Numerical simulation software.
- Open access version control
- Archiving assets according to customer needs.

We also aim to provide the highest levels of data protection and privacy concerning the data of our clients and all other partners with whom we interact.

We aim to guarantee the complete security of all our hardware and software systems.

Actions

We do this by:

Developing in-house tools around open-source software and publishing/archiving these products.

Embedding best practices concerning open data, data protection and security in our core work ethic, individual projects and our training.

Ensuring that managers and staff understand and operate by the principles outlined above, and understand how to report breaches or concerns.

Working only with vendors that provide clear provenance in data pipelines, GDPR compliance, and best in class cyber security.

Accountability

Our Open Data, Privacy and Cyber Security Policy is updated and signed off annually by the board of directors.

Concerns and/or breaches are reported directly to our Chief Technical Officer, and are considered immediately by an exceptional meeting of the board.

This policy forms part of a suite of policies designed to ensure that we meet the highest standards for sustainable insights and research standards.

James Evans

CEO

21st February 2023