Lowell's approach to: **Protecting data**

Lowell is trusted by its customers to store, manage and process their data safely. This trust must be earned; something we do primarily through our everyday actions but also by giving complete transparency to our commitments, as conveyed by our privacy notices available on our customer websites. For a quick view, see our UK Privacy Promise for our commitments relating to how we will collect, use, maintain, store and protect customer information.

We take the topic of data protection very seriously. It is a fundamental human right and it is important to us that the data we are entrusted with is handled respectfully and compliantly.

Our approach to collecting using and storing customer data (SASB SV-PS-230a.2) is covered across a range of policies that align to the relevant regulatory requirements, legislation and standards within the regions where we operate, such as data protection law, to set out our overarching approach.

Policies include:

- **Data Governance**
  Covering the way we manage and use our data
- **Information Risk (data protection)**
  Covering compliance with the data protection legislation
- **Information Security**
  Covering how we ensure data is kept safe and secure
- **Information Classification and Handling Policy and Guidelines**
  Covering how different types of information should be treated
- **Information retention**
  Covering how long different types of information can be kept for

Lowell's approach to: **Protecting data**

And are supported by a range of procedures and controls covering:

- Access control
- Anonymisation and pseudonymisation
- End user-oriented topics including acceptable use of assets, clear desk and clear scree, information transfer, mobile devices and teleworking and restrictions on software installations and use
- Protection from malware
- Management of technical vulnerabilities
- Cryptographic controls
- Communications security
- Issue identification, escalation, and management
- Storing and sharing information

Policies are communicated to colleagues to ensure that they understand their responsibilities and all colleagues are provided with training on data security and privacy within six months of joining, with refresher training provided on an annual basis.

Only authorised users can securely access and share information in order to perform their roles and these users receive specific training about their information security responsibilities.

Information security responsibilities are also included in contracts of employment, role descriptions, personnel specifications and personal development plans where appropriate.

Due to its prominence, the topic of good data practices is captured across three of Lowell's top ten residual risks: data privacy, data management, and information and cyber security (see Risk Management Overview).

We make sure our contractual and legal obligations are met and work to continually improve our procedures, including learning from any incidents which may take place.