Assurity Consulting has a legal and moral duty to protect all data and information that it collects, processes, holds, stores, sends and receives. This includes data and information in both hard and soft copy formats and that is sent or received by post, courier or electronically.

Data Protection – the safeguarding of personal data

We need to control and process data both directly as well as through and on behalf of trusted third party partners. As a responsible business we apply and are able to demonstrate compliance with the following principles to our control and processing of personal data:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- processed in a way that is adequate, relevant and limited to what is necessary;
- maintained to ensure it is accurate and where necessary kept up to date; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

We take reasonable steps to ensure that third parties who process data on our behalf also apply and are able to demonstrate compliance with the above principles.

Privacy – the processing of personal data

Where we are controlling data we will provide clear and transparent information to data subjects in the form of privacy notices. To avoid unnecessary complexity and irrelevant information we will maintain tailored privacy notices for different categories of data subjects, including but not limited to: customers, potential customers, suppliers, employees, and website visitors. These privacy notices will be supplied at the time of, or within a reasonable time of obtaining the data.

Information Security – the protection of information

We will protect our customers, suppliers, employees and other stakeholder's reputation by ensuring their information does not get into the wrong hands.

Where information is held or stored, we will make sure:

- It is kept in a locked building that is protected by camera's and alarmed when the building is unoccupied;
- It is only viewed by those people with the appropriate authority; and
- It is disposed of using methods that are appropriate for the security of the information.

Where information is held, stored, sent or received in a soft copy format, we will make sure:

- It is protected using IT products and methods that are appropriate for the security of the information;

Where information is sent or received in a hard copy format, we will make sure:

- It is protected using methods that are appropriate for the security of the information.

We will audit our own processes periodically to demonstrate compliance with this policy, and to identify and where reasonably practicable act upon improvements that these audits may identify.

This policy will be reviewed at least once every two years.

Signed **Dated: 11 February 2025**
Keith Vigar
Managing Director