

Data Protection Policy

Bristow & Sutor is fully committed to compliance with the requirements of the Data Protection Act 1998 ("the Act"). We will therefore follow procedures that aim to ensure that all employees, contractors, agents, consultants and partners who have access to any personal data held by or on behalf of Bristow & Sutor, are fully aware of and abide by their duties and responsibilities under the Act.

Bristow & Sutor, acting as custodians of personal data - recognises its moral duty to ensure that all such data is handled properly and confidentially at all times, irrespective of whether it is held on paper or by electronic means. This covers the whole lifecycle, including:

- The obtaining of personal data;
- The storage and security of personal data;
- The use of personal data;
- The disposal / destruction of personal data.

Bristow & Sutor also has a responsibility to ensure that data subjects have appropriate access - upon written request - to details regarding personal information relating to them. This is done in consultation with clients, where the client is the data controller.

In order to operate efficiently, Bristow & Sutor has to collect and use information. This information may include information about members of the public, current, past and prospective employees, clients and customers, and suppliers. This personal information must be handled and dealt with properly and in accordance with our Data Protection Notification regardless of how it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

Bristow & Sutor regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the company and those with whom it carries out business. Bristow & Sutor will ensure that it treats personal information lawfully and correctly.

To this end Bristow & Sutor endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

PRINCIPLES OF DATA PROTECTION

The Act stipulates that anyone processing personal data must comply with **Eight Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **"sensitive" personal data**.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

HANDLING OF DATA

Bristow & Sutor will, through appropriate management:

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

In addition, Bristow & Sutor will ensure that:

- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;

All managers and staff will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Personal data that is destroyed, is shredded in the confidential waste bins provided.