ASTONS ACCOUNTANTS
AND ADVISORS LIMITED

Astons
ACCOUNTANTS

PRIVACY POLICY STATEMENT

Astons acknowledges and accepts its statutory responsibilities and aims to secure and maintain the confidentiality and security of its employees and clients.

All clients and employees of Astons shall be made aware of the requirements of this Privacy Policy Statement and shall be required to meet its objectives insofar as they can be expected so to do.

Astons will aim not only to comply with the relevant, prevailing, statutory responsibilities, including the General Data Protection Regulations (GDPR), but will also seek to prevent any breaches of the firm's confidentiality or privacy arrangements and any repercussions arising from any such breaches, and all personnel will be expected to bear this in mind at all times and adopt a similar approach to individual roles.

The promotion of the privacy and confidentiality of all employees and clients is fundamental to the policies and activities of the operation. Therefore, all activities will be carried out as securely and efficiently as possible, with a view to maintaining the privacy and confidentiality of everyone associated with Astons, to contribute to the success of the business in meeting its privacy objectives.

The commitment of the business to these aims will be demonstrated by the facts that it will:-

1. take all reasonable steps to protect the privacy and confidentiality of its clients and personnel whilst at work and that of all other parties who may be affected by its operations;
2. take all reasonable steps to avoid a breach of the privacy policy;
3. take all reasonable steps to avoid any harm befalling any client or employee which might occur as a consequence of any breach of the privacy policy, mainly being careful and responsible in implementing activities, procedures and any changes thereto;
4. provide systems of work that are as secure and confidential as possible;
5. ensure that risk assessments of all appropriate activities are conducted and documented with systems being put, and kept, in place to monitor and control risk to a satisfactory level.

……Page 1 of 4….continued……..

6. Ensure that all personnel involved in the implementation and maintenance of this policy and any/all persons affected by it are aware of it, understand it and are committed fully to it;

7. ensure that this policy statement is displayed at each business facility and/or site;

The intention of the business to support the above policy aims and commitments will be supported by the facts that it will:-

A. provide all available resources to ensure the full implementation of this policy;

B. provide sufficient supervision, information, instruction and training to ensure the privacy of personnel and clients who may be affected by its operations;

C. set up systems, procedures and working practices to ensure that all activities are carried out in a confidential and responsible manner;

D. monitor compliance with this policy and all related/supporting working practices, systems and procedures, all of which should/will be reviewed regularly to ensure the maintenance of the highest possible practicable standards concerning privacy and the security of data;

All personnel of the business are expected to support the above policy aims and commitments and to demonstrate that they are committed to privacy issues so that management and personnel can work together to optimise the ideas and improvements generated and the implementation of all existing aspects of the policy as well as any improvements to it. Indeed, the Data Protection Acts and General Data Protection Regulation requires personnel to take reasonable care to ensure their own privacy, as well as that of others, whilst at work.

Therefore, all personnel must:-

(i) take all reasonable steps to protect the privacy of themselves, other employees, members of the public and any/all other parties, who may be affected by their activities/actions whilst at work;

(ii) Immediately refer to superior personnel, any aspect of their work, their conditions, their equipment or their working environment which has, or may, become a risk to the privacy and confidentiality of anyone;

(iii) Immediately refer to superior personnel, any aspect of their work, their conditions, their equipment or their working environment or their remit at work for which they are not aware of the relevant privacy requirements;

...*continued*.....

Personal information is taken as being/including:-

Name(s)
Address(es)
Telephone numbers (landlines and mobile devices)
Email addresses
Date of birth
Tax Reference number
National Insurance number
Businesses (particulars and related performance/finances)
Employment (particulars and related finances)
Pensions (particulars and related finances)
Bank accounts (particulars and related finances)
Investments (including properties - particulars and related finances)
Relatives' particulars
Interaction with government department or agencies

Personal information can be communicated:-

Verbally,
In writing,
Via websites
Via email
Via social media
Via mobile/portable communication devices ('phones, laptops and tablets)

Use of personal information is taken as being/including:-

All communication with third parties will be in line with what you expect of your past and/or normal/foreseeable dealings with us. If any unexpected use of the information arises, we will only ever act in what we believe to be your best interests and, wherever possible, we will inform you and seek to obtain your expressed consent.

Holding information on our systems for ongoing reference,
Communication with you and any authorised third party,
Communication with Her Majesty's Revenue & Customs (HMRC)
Communications with Companies House (if applicable)
Communications with your bank (if authorised)
Communications with your pension provider (if applicable and authorised)
Communications with your financial advisor (if applicable and authorised)

Third party access to personal information:-

Generally, we do not allow any other entities to access personal information without your expressed consent.

However, in our 'normal course of our business' we run and maintain computerised systems with software running on them. Our systems have secure remote access for engineers to deploy and, on occasions we need to grant software providers remote access to cure problems, deal with difficulties and/or failures or 'glitches'.

Some personal information may be accessible to them, but we do our best to minimise this and all such providers are fully compliant themselves with Data Protection legislation.

...*continued*.....

Destruction of personal information:-

All documents or records containing any personal information that are no longer required and securely shredded and/or destroyed.

Access to personal information:-

You have a right of access to information we hold on/for/about you and we will respond to any/all requests for such information as quickly and completely as possible.

Storage of personal information:-

Personal information is stored (physically, on paper or files/books/records) and electronically after you cease to be a client, partly in case of retrospective enquiries from you, your advisors and/or government agencies, including HMRC. Records are generally held for (at least) 7 years. After this time we reserve the right to delete any such information and destroy any related records at our convenience, but you may request deletion and/or destruction (or collection) (and confirmation thereof) at any time.