DATA PROTECTION POLICY

In the course of your work you may come into contact with and use confidential personal information about people, such as names and addresses or even information about customers' circumstances, families, health and other private matter. This policy helps you ensure that you do not breach the Data Protection Act 1988, which provides strict rules in this area. If you are in any doubt about what you may or may not do, seek advice from your line manager. If you are in doubt and cannot get in touch with him/her, do not disclose the information concerned.

Amtico hold personal data about you. You have consented in your employment contract to the data being used as set out in the contract. If this data changes, you should let us know so that our records can be updated.

The Data Protection Act 1998 requires that eight data protection principles be followed in the handling of personal data. These are that personal data must:

- Be fairly and lawfully processed;
- Be processed for limited purposed and not in any manner incompatible with those purposes;
- Be adequate, relevant and not excessive;
- Be accurate;
- Not be kept longer than is necessary;
- Be processed in accordance with individuals 'rights;
- Be secure and
- Not be transferred to countries without adequate protection.

"Personal Data"

The Data Protection Act 1988 applies only to information that constitutes "personal data". Information is "personal data" if it:

- Identifies a person, whether by itself, or together with other information in the organisation's possession, or is likely to come in its possession; and
- Is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical nature.

Consequently, automated and computerised personal information about employees held by its employers is covered by the Act. Personal information stored physically (for example, on paper) and held in any "relevant filing system" is also covered. In addition, information recorded with the intention that it will be stored in a relevant filing system or held on computer is covered.

A "relevant filing system" means a well-structured manual system that amounts to more than a bundle of documents about each employee filed in date order, i.e. a system to guide a searcher to where specific information about a named employee can be located easily.

The following personal data about you will be kept by Amtico:

- Payroll data;
- Performance records;
- Address & emergency contact details;
- Pensions & tax related data.

1.0 The use of Personal information

The Data Protection Act 1998 applies to personal information that is "processed". This includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and, finally, disposing of it.

"Sensitive Personnel Data"

"Sensitive personal data "is information about an individual's :

- Racial or ethnic origin;
- Political opinion;
- Religious beliefs or other beliefs of a similar nature;
- Trade union membership (within the meaning if the Trade Union and Labour Relations (Consolidation) Act 1992);
- Physical or mental health or condition;
- Sex life;
- Commission or alleged commission of any criminal offence; and
- Proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings of the sentence of any court in such proceedings.

Amtico will not retain sensitive personal data without the express consent of the employee in question.

Amtico will process sensitive personal data, including sickness and injury records and references, in accordance with the eight data protection principles If Amtico enters into discussions about a merger or acquisition with a third party, the organisation will seeks to protected employees; data in accordance with the protection principles.

2.0 Personnel Files

An employee's personnel file is likely to contain information about his/her work history with the organisation and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal information about the employee including address details and national insurance number.

There may also be other information about the employee located within Amtico, for example in his/her line manager's inbox or desktop; with payroll; or within documents stored in a relevant filing system.

Amtico may collect relevant sensitive personal information from employees for equal opportunities monitoring purposes. Where such information is collected, Amtico will anonymise it unless the purpose to which the information is put requires the full use of the individual's personal information. If the information is to be used, the organisation will inform the employees on any monitoring questionnaire of the use to which the data will be put, the individuals or posts within the organisation who will have access to that information and the security measures that the organisation will put in place to ensure that there is no unauthorised access to it.

Amtico will ensure that personal information about an employee, including information in personnel files, is securely retained. Amtico will keep hard copies of information in a locked filing cabinet. Information stored electronically will be subject to access controls and password and encryption software will be used where necessary.

Where laptops are taken off site, employees must follow Amtico's IT policies relating to the security of information and the use of computers for working at home.

3.0 Data subject access requests

Amtico will inform each employee of:

- The types of information that it keeps about him/her;
- The purpose for which it is used; and
- The types of organisations that it may be passed to, unless this is self-evident (for example, it may be self-evident that en employee's national insurance number is given to HM Revenue & Customs).

An employee has the right to access information kept about him/her by Amtico, including personnel files, sickness record, disciplinary or training record, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the employee.

Amtico will respond to any data subject access request within 40 calendar days.

Amtico will allow the employee access to hard copies of any personal information. However, if this involved a disproportionate effort on the part of Amtico the employee shall be invited to view the information on-screen or inspect the original documentation at a place and time to be agreed by Amtico.

Amtico may reserve its right to withhold the employee's right to access data where any statutory exemptions apply.

4.0 Correction, updating and deletion of data

Amtico has a system in place that enables employees to check their personal information on a regular basis so that they can correct, delete or update any data. If an employee becomes aware that the Amtico holds any inaccurate or irrelevant or out-of-date information about him/her, he/she must notify the HR department immediately and provide any necessary corrections and/or updates to the information.

5.0 Data that is likely to cause substantial damage or distress

If an employee believes the processing of personal information about him/her is causing, or is likely to cause, substantial and unwarranted damage or distress to him/her or another person, he/she may notify in writing to Human Resources to request the organisation to put a stop to the processing of that information.

Within 21 days of receiving the employee's notice, Amtico will reply to the employee stating either:

- That is has complied with or intends to comply with the request; or
- The reasons why it regards the employee's notice as unjustified to any extent and the extent if any, to which it has already complied or intends to comply with the notice,

6.0 Employees obligations regarding personal information

Where Amtico give you code words or passwords to be used before releasing personal data, for example by telephone, you must ensure that you follow our requirements strictly. You may not give information about a family member to someone else form the same family.

If you access another employee's records without authority, this will be treated as gross misconduct and is a criminal offence.

In relation to emails and faxes, you should follow the guidance in the internet and email policy, as well as the guidance set out in this policy.

Pay particular attention to the risks of transmitting confidential employee information by email or fax:

- Transmit information between locations only if a secure network or comparable arrangements are in place or if, in the case of email, encryption is used.
- Ensure that all copies of email and fax messages received by managers are held securely.
- Amtico provides a means by which managers can effectively expunge emails that they receive or send from the system and you are responsible for doing so.
- Amtico draws your attention to the risks of sending confidential, personal information by email or fax.
- Ensure that the information systems' security policy properly addresses the risk of transmitting employee information by email.
- Where information is disposed of, employees should ensure that it is destroyed.
- Hard copies of information should be confidentially shredded.
- Where an employee is required to disclose personal data to any other country, he/she must ensure first that there adequate safeguards for the protection of data in the host country.

7.0 Consequences of non-compliance

All employees are under an obligation to ensure that they have regard to the eight data protection principles (see above) when accessing using or disposing of personal information. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's records without the requisite authority. Amtico will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

8.0 Transferring of Data

Your own personal data may be sent to our subsidiaries abroad where this is necessary to post you abroad or otherwise employ you in another of our offices.

If Amtico sells all or part of its business, it may provide personal data about you to any prospective purchaser in the course of negotiations. So far as possible such data will be provided in an anonymous form and if this is not possible the prospective purchaser will be required to keep the information confidential. We will transfer your personal data on any transfer or dale following within the terms of the Transfer of Undertakings (Protection of Employment) Regulations 1981.

9.0 Monitoring Calls and emails

Amtico monitor emails and telephone calls but strictly in accordance with what is permitted under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. You have consented to this by a term in your employment contract.