Data Protection Policy

Data Protection Policy

Introduction

Norwood UK needs to keep certain information about its employees and other users to allow it to monitor performance, achievements, and health and safety, for example. It also needs to process information so that staff can be recruited and paid, courses organised and legal obligations to customers complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Norwood UK must comply with the Data Protection Principles, which are set out in the Data Protection Act 1998.

In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Norwood UK and all staff or others who process or use any personal information must ensure that they follow these principles at all times.

Issue Date 08/03/2017
Issue 1
Document No: 026
Uncontrolled when copied

In order to ensure that this happens, Norwood UK has developed the Data Protection Policy.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Norwood UK from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to Norwood UK in connection with their employment is accurate and up to date.
- Informing Norwood UK of any changes to information, which they have provided, ie changes of address.
- Informing Norwood UK of any errors or changes in staff information. Norwood UK cannot be held responsible for any such errors unless the staff member has informed Norwood UK of them.

If and when, as part of their responsibilities, staff collect information about other people, (ie about other staff, opinions about ability, references to client information, or details of personal circumstances), they must comply with the guidelines for staff (Appendix 1).

Data Security

All staff are responsible for ensuring that:

- Any personal data, which they hold, is kept securely, for example:
  - Kept in a locked filing cabinet; or
  - in a locked drawer;
  - if it is computerised, be password protected; or
  - kept only on disk, which is itself kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

Staff Obligations

Staff must ensure that all personal data provided to Norwood UK is accurate and up to date. They must ensure that changes of address, etc are notified to the HR Department.

Staff who use Norwood UK's computer facilities may, from time to time, process personal data. If they do so they must notify HR.

Rights to Access Information

Staff and other users of Norwood UK have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should contact HR.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing.

Norwood UK will make a charge of £10 on each occasion that access is requested.

Norwood UK aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days.

Subject Consent

In many cases, Norwood UK can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to Norwood UK processing some specified classes of personal data are a condition of acceptance of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974.

Some jobs will bring staff into contact with children, including young people between the ages of 16 and 18 and the elderly and venerable. Norwood UK has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. Norwood UK also has a duty of care to all staff and must therefore make sure that employees and those who use Norwood UK services and facilities do not pose a threat or danger to other users.

Therefore, all prospective staff will be asked to consent to their data being processed when an offer of employment is made. A refusal to sign such a form may result in the offer being withdrawn.

Criminal Records Bureau (CRB/DBS) disclosure

We are required by law to undertake CRB/DBS checks in respect of our Engineers because of the nature of where we work – for example, schools and hospitals. A number of our customers require copies of CRB checks in order to comply with their own rules and regulations.

Accordingly, where requested, we intend to provide copies of CRB checks.

Because disclosing the CRB checks will involve the processing of sensitive personal data about you (for the reasons and purposes set out above) we need your consent under the Data Protection Act 1998.

Staff may therefore be requested to complete a CRB/DBS check when you first start. You will always be notified if a form is being sent for approval. A standard check will be paid by the Company. We reserve the right to deduct this amount from your final salary should you decide to terminate your employment before twelve weeks.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's criminal convictions, race and gender and family details. This may be to ensure Norwood UK is a safe place for everyone, or to operate other Norwood policies, such as the sick pay policy or equal opportunities policy. Norwood UK will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes or disabilities. Norwood UK will only use the information in the protection of the health and safety of the individual, but will need consent to process for example, in the event of a medical emergency. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, Staff will be asked to give express consent for Norwood UK to do this. Offers of employment may be withdrawn if an individual refuses to consent to this, without good reason.

The Data Controller and the Designated Data Controller

Norwood UK as a Limited company is the data controller under the Act, and all Norwood is therefore ultimately responsible for implementation. However, the designated data controller will deal with day to day matters.

Norwood UK has designated Mrs Jo Shuttlewood (Director of HR) to act as Data Controller and as Data Protection Officer. Any query relating to the implementation within Norwood UK of the Data Protection Act 1998 should be referred to Mrs Jo Shuttlewood.

Retention of Data

Norwood UK will keep some forms of information for longer than others. Data on staff, including any information on health, race or disciplinary matters, will be destroyed after 10 years but a skeletal record will be retained.

Norwood UK will need to keep central personnel records indefinitely. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

Conclusion

Compliance with the Data Protection Act 1998 is the responsibility of all members of Norwood UK. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Norwood facilities being withdrawn, or even a criminal prosecution.

Signed for and on behalf of the company

Jo Shuttlewood – HR Director

Issue Date 08/03/2017
Issue 1
Document No: 026
Uncontrolled when copied