Data Protection Policy
July 2018

Policy Group: Support Policies
Policy Number: 7.51
Policy Title: Data Protection Policy
Author: Quality Department
Date and current version: July 2018
Review Date: January 2019

This document is issued and controlled by the Quality Department and can only be modified after proposed modifications have been accepted by the Senior Management Team.
The latest version will be maintained by the Quality Department and held on the Products & Services shared drive

Purpose

The company is registered with the Data Protection Registrar (ICO) in order to comply with the storage and/or processing of personal information, and is also known as the Data Controller. The company will monitor its storage and information processes at frequent intervals in accordance with current legislation and to ensure its continued compliance within the remit of its Data Protection Registration. Any information that is found to be materially incorrect will be amended as soon as practicable or destroyed.

Nordic Products & Services collects personal information about people with whom it deals with in order to carry out its business and provide its services.

Such people include learners, employees (present, past and prospective), suppliers and other business contacts. The information includes name, address, email address, date of birth, private and confidential information, sensitive information. In addition, we may be required to collect and use certain types of such personal information to comply with the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 1998.

The lawful and proper treatment of personal information by Nordic Products & Services extremely important to the success of our business and in order to maintain the confidence of our service users and employees we ensure that Nordic Products & Services treats personal information lawfully and correctly.

Scope

All Employees/Associates

Data Protection Principles

Nordic Products & Services fully supports and complies with the eight principles of the Act which are summarised below;

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained/ processed for specific lawful purposes
3. Personal data held must be adequate, relevant and not excessive
4. Personal data must be accurate and kept up to date
5. Personal data shall not be kept for longer than necessary
6. Personal data shall be processed in accordance with rights of data subjects
7. Personal data must be kept secure

8. Personal data shall not be transferred outside the European Economic Area (EEA) unless there is adequate protection

Staff duties

Employees are expected to:

- Acquaint themselves with, and abide by, the Data Protection Principles;
- Read and understand this policy document;
- Understand how to conform to the standard expected at any stage;
- Understand how to conform to the standard expected in relation to Safeguarding data subject's rights (e.g. the right to inspect personal data) under the Act;
- Understand what is meant by 'sensitive personal data', and know how to handle such data
- Understand that breaches of this Policy may result in disciplinary action, including dismissal

As an employee for Nordic Products & Services you deal with sensitive/ confidential/ personal information relating to our customers, learners or employees.

If disposing of any information which may be sensitive/ personal etc. it should be disposed of correctly.

No confidential/ personal or sensitive information should ever be disposed in a main waste bin. Instead it should be disposed in one of the confidential 'Shred It' waste bins within the building.

As we have a large amount of guests and learners in the building it is imperative confidential and sensitive information is not seen by them. For example information could be easily visible on your computer/laptop screen and any information on desks could be seen by anyone passing. Therefore it is good practice to 'minimise' all on screen documents or, better still, to lock your workstation if you are leaving it unattended for any period of time. Similarly, all sensitive / confidential information should be turned face down so not to be visible.

Company Responsibilities

The company shall use any data it holds to ensure it can monitor and comply with any current legislation, particularly in terms of equal opportunities and non-discrimination. Where the company holds any employee's personal data, it shall check this data from time to time to ensure that it remains accurate. This shall be carried out on a regular basis by contacting each employee to confirm the details held on file.

Employees who becomes aware of a material change to their circumstances; such as their personal details/maiden names/aliases, home address, next of kin or any contact phone numbers; is required to notify the Corporate Services Department as soon as practicable.

The company may also collect and store data on any other persons associated with the carrying out of its business, or as part of its recruitment and/or training programme. Wherever possible, any information stored will be verified as correct and will be regularly audited for its accuracy.

DATA SECURITY, CONFIDENTIALITY AND PRIVACY

All data or information sorted or processed on the organisation's systems or transmitted within or from the organisation (e.g. e-mail, voice-mail) is the property of the organisation and may be accessed, read or monitored accordingly. Any employee with access to company IT resources must ensure the confidentiality and appropriate use of any accessible data, by being aware of the security needs of equipment where such information may be held or displayed, as well as the protection of any access rights, such as passwords.

All employees are required to abide by the privacy rights of all other employees regarding the disclosure of personal information, as required by current legislation. It should also be noted that disclosure of confidential information to unauthorised persons or entities, or the use of such information for self-interest or advantage, is prohibited; as is access to non-public areas of any network drive. Breaches will be treated severely under the company disciplinary rule

DATA BREACH OR DATA LOSS

Any member of staff who is responsible for holding any Personal Data as defined within this policy (regardless of the media on which it is held), has a responsibility to consider the security of that data at all times it is in their possession.

An example of this would be to ensure that all the necessary system protections are in place such as anti-virus software and passwords on a laptop, or that filing cabinets are securely locked, in order to prevent unauthorised access to the data. In addition positive steps should be taken by the employee to prevent the physical loss of the data, for example losses arising from leaving paperwork or a laptop on the back seat of a car, or on a train seat.

If any data is lost, or believed to be lost, then the employee MUST report this to a Director of the Company as soon as practicable.

PRIVACY

All users of the company's IT resources are advised to consider the open nature of information disseminated electronically, and should not assume any degree of privacy or restricted access to such information. The company strives to provide the highest degree of security when transferring data, but cannot be held responsible if these measures are circumvented and information is intercepted, copied, read, forged, destroyed or misused by others.

Though it is not the intention of the company to continuously monitor Internet and e-mail communications, or access data files held by an individual; the company reserves the right to do so at any time. The company has the right to read and/or delete any data stored on company owned or leased equipment. All employees must be aware that they therefore have no right of privacy in respect to Internet and e-mail communications, or stored data, utilising company owned or leased equipment.

However, it should be noted that the company would not normally access an employee's data or communications without first requesting permission to do so. Although, in the event of an internal disciplinary investigation, or on the request by a Government Agency, or as a result of litigation against the individual and/or company, any e-mail or data files may be locked and/or copied to prevent destruction and loss of information. In such cases, the company may revert to its right to view any data held without first requesting the permission of the individual concerned.

The Right to Access Personal Data.

Nordic Products & Services recognises that under the Data Protection Act 1998 any data subject has a right to request access to his/her personal data. Such a request is known as a "Subject Access Request" (SAR).

All subject access requests should be addressed to the Director of Operations. Nordic Products & Services will charge a £10.00 administration fee per subject access request.

Nordic Products & Services will not process a request until it is in receipt of the request in writing, proof of identity and the £10.00 administration fee. Once Nordic Products & Services has received all 3 items, a 40 day response time will begin. The clock will stop if Nordic Products & Services contacts the data subject to request additional information in order to process the request. The clock will start again once that additional information is received.

20/7/18

Peter Robinson

CEO/Managing Director