Yafforth Road, Northallerton, North Yorkshire, DL7 0LQ,
Phone. 01609 770269, Fax 01609 770056, Email: northdalhort@aol.com,
Reg. Charity No. 1142535 VAT Reg. No. 886673068

NORTHDALE HORTICULTURE POLICIES AND PROCEDURES

DATA PROTECTION

Policy Statement

Northdale Horticulture aims to protect the rights of the individual at all times. The organisation endorses fully the statements and the intent of the Data Protection Act (1998).

Scope

This policy and procedure encompasses all aspects of the Charity's activities as an employer and service provider.

Staff Responsibilities

The Data Controller for Northdale Horticulture is the Company Secretary, who is to ensure that ~~this~~ the Charity's policies~~y~~ and procedures are adhered to, and to monitor adherence. The General Manager will nominate an IT Supervisor who will be responsible for the day-to-day management of all of the Charity's IT systems.

Definitions

Personal Data: ~~means~~ data (manual or electronic) which relates to a living individual, who can be identified from that data (or from that data and other information that is in the possession of, or is likely to come into the possession of, the data controller).

Formatted: Font: Bold

Data: ~~means~~ information that is being processed automatically or is recorded with the intention that it should be processed automatically. Any manual data that forms part of an "accessible record" is also included in this definition within the Data Protection Act.

Formatted: Font: Bold

Data Controller: ~~means~~ a person who determines the way in which any personal data is to be processed.

Formatted: Font: Bold

Electronic or Computer Data: ~~– means~~ data that is being processed by means of equipment operating automatically in response to instructions given for that purpose.

Employee: ~~– means both~~ paid Staff and Volunteers, including Trustees.

Service User: ~~r – means both~~ the Service User or Trainee and their Recognised Carer.

Recognised Carer: ~~– A Recognised Carer is~~ the person who has either been identified to Northdale Horticulture as such on the Service User's admission application form, or by Social Services or other such agency.

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Procedure

Notification

Any time that data about an individual person is held manually or electronically, it must be:

- In accordance with the Charity's Confidentiality, Record Keeping and Access to Information Policy.
- In accordance with the 8 principles of the Data Protection Act.
- Available to be seen by the person named.

Processing

All Employees, Service Users and Recognised Carers must be sure that data held on manual and computer files about individuals is:

- Processed fairly and lawfully.
- Accurate and up-to-date.
- Used only for defined purposes.
- Kept private.
- Kept only for as long as it is useful.
- Relevant and not excessive.

Disclosure

- The primary principle on which disclosure of information should be based is that any disclosure should be on 'a need to know' basis.
- The disclosure of personal information always requires the permission of the subject of the enquiry.
- The identity of any person requesting information about themselves or a third party must be verified, and in the case of a third party, that the person receiving the information is properly authorised to receive it.
- Before disclosing personal information to a third party, the reason the data is required and to whom that party intends to disclose it should be verified. Personal

information should only be disclosed when the disclosure complies with the above and the Data Protection principles.
- If an individual is aware of any data held or disclosures made that break the data protection principles, this must be reported to the Chairman of the Management Committee or the General Manager in order that the breach may be addressed.

Policy on Authority to Access

- The Computer Misuse Act (1990) identifies the legal framework for definition of and prosecution for unauthorised use or misuse of computers and computer systems. Whilst the Act is particularly intended to deal with unauthorised accesses from outside the organisation ("hackers"), it deals equally with unauthorised access from inside.
- It is essential that computer users understand the extent of their authority to use and access systems. ~~-~~Computers used for more than one purpose and those connected to the internal network provide the potential for access to personal, private and confidential data.
- This policy makes it the responsibility of computer users to guard and protect the personal ability to access systems ~~that~~ which only they have the authority to use.
- Computers that are being used to process confidential and financial information of a personal nature, such as salaries, must not be left logged in when unattended.
- Any employee finding that they have access to systems and data which they are not authorised to use must report this to the General Manager, in order that the access may be removed.
- Any employee with authority to access data that is no longer necessary to their work must ask for the access to be removed.~~-~~ Any employee who knows that unauthorised access is taking place must report this to the General Manger, in order that the access may be removed.
- Penalties under the Act fall into two main categories:

    - Unauthorised access – Anyone gaining access, or attempting to gain access to computer data they are not authorised to see, may face a fine of up to £2,000 or six months in prison, or both.
    - Ulterior intent or unauthorised modification – Anyone accessing data with an ulterior motive or modifying data without authorisation, may be sentenced to up to five years in prison or an unlimited fine, or both.

Data Security Policy

- All Staff must:

    - Not leave computers that are being used to process confidential and financial information of a personal nature, such as salaries, accessible when unattended. Screen Savers are to be used. ~~-~~They should be set to activate after a maximum of

5 minutes has elapsed and must be password protected in order to regain access to the system.
    - Make sure they are authorised to use the systems needed.

- The Office IT Supervisor is to ensure that:

    - New User accounts are only added to the system as instructed by the Data Controller.
    - When an employee leaves the Charity, their User account is removed from the system.

Staff Training Requirements

Members of Staff and Volunteers will receive training on Data Protection during their induction.

References

Data Protection Act 1998
Computer Misuse Act 1990

Related Policies and Procedures

Confidentiality, Record Keeping and Access to Information
IT Acceptable Use Policy

Date of last review: 23 November 2017