THE SOUTHEND ON SEA DARBY & JOAN ORGANISATION LIMITED

INFORMATION GOVERNANCE POLICY

Purpose

To describe a system that ensures The Darby & Joan Organisation meets its responsibilities for the management of information assets and resources.

Scope

- All information used by The Darby & Joan Organisation
- All information systems managed by The Darby & Joan Organisation
- Any individual using information ‘owned’ by The Darby & Joan Organisation
- Any individual requiring access to information ‘owned’ by The Darby & Joan Organisation

Rationale

Information is a vital asset and resource, both in terms of the support to individual residents and the efficient management of services and its support. It plays a key part in service governance, service planning and performance management. It is of paramount importance that information is efficiently managed; that appropriate accountability, standards, policies and procedures provide a robust governance framework for information management.

The Darby & Joan Organisation Aims

- To hold information securely and confidentially
- To obtain information fairly and efficiently
- To record information accurately and reliably
- To use information effectively and ethically
- To share information appropriately and lawfully

THE SOUTHEND ON SEA DARBY & JOAN ORGANISATION LIMITED

Responsibilities

All information used in the Organisation is subject to handling by individuals and it is necessary for these individuals to be clear about their responsibilities and for the Organisation to support appropriate awareness and training. The Organisation must ensure legal requirements are met.

To manage its obligations the Organisation will issue and support policies and procedures ensuring information is held, obtained, recorded, used and shared correctly.

Responsibilities of the Users

Users of information must:

- Be aware of their responsibilities
- Comply with policies and procedures issued by The Darby & Joan Organisation

Information Governance Framework

The Darby & Joan Organisation places importance on the confidentiality of and the organisation's security arrangements to safeguard both personal information about users, carers, volunteers and staff and commercially sensitive information necessary for the operation of the Organisation.

The Organisation also recognises the need to share information with other organisations and other agencies in a controlled manner consistent with the interests of the resident.

The Organisation believes that accurate, timely and relevant information is essential to deliver the highest quality services. As such it is the responsibility of all Managers and staff to ensure and promote the quality of information and to actively use information in decision-making processes.

Managers are expected to take ownership of and seek to improve the quality of information within their homes and are expected to ensure effective record management within their home. The Organisation will promote information quality through policies, procedures, and training.

Computer Security

Overall computer security is the responsibility of the data security officer (the Home Manager). All computers will be password protected to limit access to them. Dependent on the role applied for, job applicants will be questioned on their computer experience. All references will

be checked. Employees of all grades are permitted access only to those parts of the computer system which they need to enter in order to carry out their normal duties. Employees may access the Internet but access to certain sites eg: Social networking sites are not permitted. Employees with access to personal data are in a particularly sensitive position and must bear in mind at all times the provisions of the Data Protection Act.

Passwords must be used at all times and changed at least every 6 months or when a member of staff leaves the Organisation, whichever is sooner. Employees should not select obvious passwords. All passwords must be kept confidential. Employees must not give their passwords to other members of staff or to any person outside the Organisation. Password protected sites should be closed when finished with and computers switched off. Computers should not be left open and unattended.

The entire Organisation's software must be formally authorised by the data security officer. Regular checks should be made for viruses. No external software (USB sticks, discs etc) may be used without authorisation by both the data security officer and the employee's line manager. Misuse of computers is a serious disciplinary offence. Depending on the circumstances of each case, misuse of the computer system may be considered gross misconduct. Please refer to the disciplinary rules and procedures. Misuse amounting to criminal conduct may be reported to the police.

All breaches of computer security must be referred to the Home Manager. Where a criminal offence may have been committed the senior management team will decide whether to involve the police. Any member of staff who suspects that a fellow employee (of whatever seniority) is abusing the computer system may speak in confidence to the Home Manager.

(Please also refer to use of e-mail and internet policy & Computer Security policy)

Information Storage and Disposal

When a resident leaves the home their file will be kept 'live' for approximately 4 weeks after which time the paperwork will be archived and stored securely for a period of 3 years from date of last entry. Work diaries and communication books may hold similar information and should be kept in the same way.

It should never be necessary to take confidential residents files outside of the home. If any information needs to be taken out a copy should be made and authorisation for the information to leave the home should be sort from the Senior Carer or Home Manager. Copies of paperwork should be shredded once brought back into the home.

Filing cabinets containing confidential information should be locked at all times. When needing to access the cabinet the information should be taken out and the cabinet re-locked until this information is replaced. Under **NO** circumstances should the cabinet or information held within be accessible to anyone other than authorised staff members.

THE SOUTHEND ON SEA DARBY & JOAN ORGANISATION LIMITED

The digital sign-in system for staff and visitors stores names and mobile phone numbers for a period of time. The care manager will erase visitor information from the system (names, mobile numbers, dates and times of visits) after 90 days. Staff records on the digital system will be kept for a period of 1 year.

Confidential documents stored on a USB stick should be password protected/encrypted. It is the responsibility of the staff to ensure the safe keeping of USB stick in accordance with General Data Protection Regulations. The loss of a device MUST be brought to the immediate attention of your line manager and will be recorded as an incident.

(Please also refer to retention of records policy)

Confidentiality

Information should only be disclosed to people who need to know it. The information should be relevant, honest, factual and only sufficient to ensure the Organisations duty of care is fulfilled. The information disclosed should be proportionate to the issue being dealt with.

To take care to ensure that we do not to pass on information about a resident unless we have the written third party information sharing agreement in place

Telephone calls of a confidential nature will be made in an area private enough so to avoid anyone being able to over hear the conversation.

(Please also refer to confidentiality policy)

Data Protection

(see Data Protection Policy)

Staff Training

All staff are made aware of information governance at induction, through our staff handbook and relevant policies are regularly reviewed with the staff team to further develop knowledge on the subject. Where necessary and if identified through supervision and support, outside training will be sourced to develop the staff member further.

This policy is reviewed annually.