CCT Community Enablement Team
Now You Can

Policy No: 060	Authorised: A Parker/ J Wynn	Date: 15/01/2018

INFORMATION SECURITY

Policy Statement

Information processing is a large part of our business processes and we must protect the integrity of our data and perhaps more crucially the people involved in the day to day handling and management of the data.

The Policy

Information security is primarily about people but is facilitated by the appropriate use of technology. Important factors are:

- Assurance that information is managed appropriately, securely and in a consistent and corporate way
- Assurance that we as an organisation provide a secure, safe environment for the management of information used in delivering our services
- Assurance that information is accessible only to those authorised to have access
- Clarity over rules and responsibilities of staff in regard to information security
- Ensure that risks are identified and appropriate controls are implemented and documented
- Regulators are identified and appropriate access to information is given in a timely and lawful manner e.g. Care Quality Commission, local authority contract monitoring

It is important therefore that all staff understand and comply with all requirement of this policy in their day to day handling of information. Further, what procedures, standards or protocols exist for the sharing of information with others; and perhaps most importantly, how to report as suspected breach of information security, intentionally or otherwise.

Within this organisation the following is in place.

Access to I.C.T facilities are restricted to authorised users who have business needs to use such facilities, which are password protected.

Access to written data such as personal or Service User information is on a need to know basis.

Equipment inventories are established and reviewed at regular intervals.

Computer and Network management is regularly reviewed including back-up off site where applicable.

Regular virus checks are in place to prevent malicious incident.

No staff are allowed to install software by any means, without the approval of the Registered Manager.

Regular monitoring of I.C.T. use (including telephone communications) is available to the organisation and is accessed via the I.C.T. administrator.

Related Policies

Co-operating With Other Providers

Confidentiality

Data Protection

Information Sharing Protocol

Record Keeping

Training Statement

This is covered during Induction under good governance and staff are aware of their responsibilities from the beginning of their employment, particularly office based staff.