mariposa elderly care CAREPORT GROUP papillon specialist care

OPSR28 CYBER SECURITY POLICY

Policy area:	Operations (Residential)
Title of policy:	OPSR28 Cyber Security
Version:	V1 – June 2020
Effective date:	24 September 2020
Approved by:	Chief Operations Officer
Approved date(s):	24 September 2020
Revision date:	As required

Scope

- **Policy Statement**
- **The Policy**
- Process Requirements
- Physical Security
- Potential or Actual Security Breaches
- Information Sharing Guidance
    - Information Sharing Principles
    - The Golden Rules
- **Related Policies**
- **Related Guidance**
- **Training Statement**

Policy Statement

The purpose of this policy is to protect, to consistently high standards, all information assets relating to Residents or Group Personnel, records written or electronic and all other corporate information, from all potentially damaging threats, internal or external, deliberate or accidental, imagined or real.

The Policy

Where information security is cited, it includes cyber security and vice versa.

Information security is primarily about people, but is facilitated by the appropriate use of technology, which is ever more sophisticated and evolving in its nature.

This policy applies to all aspects of information handling, including, but not limited to

- structured record systems – paper and electronic;
- information recording and processing systems – paper, electronic, video, photographic and audio recordings;
- information transformation systems such as fax, email, portable media, post and telephone;

The purpose of the policy is to achieve a consistent approach to the security management of information throughout the organisation, in order to enable continual business capability and to minimise the likelihood of occurrence and the impact of any information security incident or breach.

Process Requirements

Information security is paramount in maintaining and protecting the confidentiality, integrity and availability, where appropriate, to the organisation's information or data. There are 3 elements to the process:

- maintain the confidentiality of personal information including customers/residents and staff by protecting it in accordance with all legal and regulatory framework criteria.
- ensure the integrity of the organisations information by developing, monitoring and maintaining it to a satisfactory level of quality for use within the relevant activity area.
- review and implement the necessary measures to maintain availability of the organisations information systems and services, including putting in place contingency measures which ensures the minimum of disruption, should an incident or breach occur.

Physical Security

The physical security of information is the responsibility of everyone who is involved in the handling, maintaining, storage, retrieval, including any information which is shared, transmitted electronically or transported by external suppliers e.g. courier services and postal deliveries. Staff at all levels throughout the organisation must take all necessary precautions to avoid loss, theft, damage or misappropriation of information. The following good practice should be followed.

- all staff must wear I.D. badges; individuals not doing so, in non-public areas should be challenged;
- visitors must sign in, be met at reception and accompanied where appropriate;
- all doors must be properly secured and, where used, entry codes must be regularly changed to protect their integrity;
- anyone loitering or obviously out of place should be asked their purpose of visit and checked accordingly;
- in order to prevent a malware contamination, no external hardware such as USB, Memory or Recording Portable Devices can be used within the organisation, without prior approval from the IT Manager or a Director;
- management of computers and/or networks is controlled in house by the IT Manager;
- users, shall not install software, for any purpose, unless authorised to do so by the IT Manager. Those who breach this requirement may be subject to disciplinary action;
- screens should be locked when unattended even for short periods, such as toilet breaks;
- passwords should not be shared unless where that logon is intended to be part of a job role group that requires it, in this case the password is not to be shared outside of that role group. Any passwords should be changed as soon as a suspected breach or loss of control of the password is suspected. If at all unsure if something has occurred or something is seen that raises a concern, then contact the IT Manager for assistance;
- disposal of equipment is allowed only by the IT Manager;
- all IT and telephone equipment must be purchased via the IT Manager;
- any stolen or damaged IT equipment must be reported to the IT Manager within 24 hours of the discovery;
- secure transfer of files and documentation whether physically or electronically, must be properly recorded and approved by the relevant Data Controller;
- should a legitimate need arise for a non-routine transfer of information, a risk assessment must be undertaken first to determine the most secure transfer process e.g. courier, by hand only, etc. Any such transfer must be approved by the relevant Data Controller.
- adequate and appropriate monitoring of information that is held and its use, should be undertaken at least annually, as part of the audit cycle;
- record management systems, policies and procedures should be followed at all times, within the information chain;
- paper information is particularly vulnerable, for instance, person identifiable, sensitive personal information should be locked away when desks are left unattended;
- a clear desk routine should be followed, with a final check in place at the end of the working day, which includes paper vulnerability and computer security;
- computers should be turned off at the end of the day to provide the best protection from unauthorised access;

- If you are wanting to bring your own device (BYOD), phone or tablet, to access company email and SharePoint files then there are some conditions to cover this as follows:

    - Any new device you are wanting to use needs to be approved by the IT Manager
    - All devices must be protected by at least a 4 digit unlock PIN and fingerprint or facial recognition where available
    - The device must be set to automatically lock after 2 minutes of inactivity and require the PIN/fingerprint/facial recognition
    - Where available, the device should have device level encryption enabled
    - You accept that by connecting your own device to company services that the organisation has the ability to remotely wipe your device until you remove such accounts
    - You must not use any devices that have had their inbuilt protection mechanisms disabled, this is usually called “rooting” or “jailbreaking”

Business continuity is assured by continually reviewing our information systems, in particular;

- that information shall be available to properly authorised personnel as and when it is required
- relevant information security awareness and training is regularly available and accessible to staff
- all breaches of information security, actual or suspected are recorded, reported and investigated and mitigating measures put into place to prevent a re-occurrence. Please refer to the Data Breach Policy.
- sufficient hardware and software firewalls are in place to protect the network from external unauthorised access as well as internally between remote sites and head office;
- software and service based virus and malware protections in place at end user level and higher, kept up to date with the latest releases as soon as they are available;
- software updates are applied regularly to Operating Systems and software packages;
- off site backups are taken of all servers and central file stores that Careport directly manage be it on premise or within 3rd party cloud services. In the event of a disaster recovery situation this would be undertaken and manged by the IT Manager;
- while we do not actively monitor internet use there are some restrictions in place for particular content, if this content is attempted to be accessed then a log of the event is made;
- information and guidance on spotting and dealing with SPAM and potentially harmful emails is provided by the IT Manager as part of the daily support tasks or as and when a specific widespread variant of the above triggers an alert to be circulated company wide. One on one or group sessions can also be held to

help assist in identifying SPAM or potentially harmful emails with the IT Manager;
- Settings that control the flow of SPAM and potentially harmful emails in to the business are always under review

Potential or Actual Security Breaches

- all staff within this organisation are responsible for ensuring that no potential or actual security breaches occur as a result of their actions.
- on receipt of a reported breach, the data breach reporting protocol will be followed, in accordance with the Data Breach Policy.
- notifications to any Regulatory body will be part of this process, where necessary.

Risk to the business is directly linked to our capacity to remain secure and any such measures must be viewed as necessary protection against any event occurring.

A range of security measures can be deployed to address:

- the **Threat** of something damaging the confidentiality, integrity or availability of information held or systems or manual records
- the **Impact** that such a threat would have
- the **Likelihood** of such a threat occurring

Information Sharing Guidance

This clarifies information sharing for staff at all levels of the organisation. Where staff are in any doubt as to whether it is appropriate to share information, advice should be sought from the Data Protection Officer at dpo@careportgroup.com.

Information Sharing Principles

- Must have lawful authority
- Must be necessary
- Must be proportionate
- Must need to know
- Must be accountable
- Must ensure the safety and security of the information shared

We are all aware of the intense media interest particularly when things go wrong, so a balanced approach to information sharing is vital in any decision to share. In safeguarding situations particularly, it is important to ask why you wouldn’t share. All health and social care staff and partner agencies have a common law duty of confidentially within their work with Adults at risk. They also have a duty to comply with the Caldicott principles. These are a set of requirements that ensure that information regarding people who use services is treated with sensitivity to maintain its confidentiality. Information that has been provided in confidence is not normally shared or used without consent from the subject and source of such information. In all cases the main legislation which underpins the sharing of information in relation to adults at risk is:

- Common law duty of confidentiality
- Data Protection Legislation
- Human Rights Act 1998
- Freedom of Information Act 2000
- Crime and Disorder Act 1998
- Care Act 2014

It is requirement that all staff of this organisation adhere to the Golden Rules, set out below, for information sharing in all instances of information Exchange between all multi-agency partners external contacts and any request for such information will only be shared when all the Golden Rules are met.

The Golden Rules

- remember that Data Protection Legislation is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately
- be open and honest with the person, family or representative from the outset about why, what, how and with whom information will or could be shared and seek their agreement unless it is unsafe or inappropriate to do so
- seek advice, if you are in any doubt, and where this is outside of the organisation, remember confidentiality
- share with consent, where appropriate and where possible, respect the wishes of those who do not consent to share confidential information
- you may still share information, without consent, if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base such judgements on the facts of the case
- consider safety and wellbeing: base your information sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions
- adhere to all policies regarding transporting of confidential and sensitive information including staff records

Related Policies

Confidentiality

Co-operating with other Providers

Data Protection Legislative Framework (GDPR)

Data Breach

Internet, Email and Mobile Phone (Acceptable Use) - please refer to the Employee Handbook

Record Keeping

Social Media and Public Relations

Whistleblowing

Related Guidance

- The National Cyber Security Centre (NCSC). www.ncsc.gov.uk
- The National Security Strategy 2016 – 2021 www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
- The Information Commissioner's Office (ICO). https://ico.org.uk/
- HSCIC now NHS Digital www.gov.uk/government/organisations/health-and-social-care-information-centre http://content.digital.nhs.uk/
- Cyber Aware www.cyberaware.gov.uk
- Cyber Essentials (CE) www.cyberessentials.ncsc.gov.uk
- Get Safe Online www.getsafeonline.org
- Action Fraud www.actionfraud.police.uk
- ISO/IEC 27001 – Information Security Standard. www.iso.org/isoiec-27001-information-security.html
- ISO/IEC 27002 - Security techniques - Code of practice for information security controls www.iso.org/standard/54533.html
- ISO/IEC 27005 - Information Security Risk Management www.iso.org/standard/56742.html

- ISO/IEC 22301 – Business Continuity Standard. www.bsigroup.com/en-GB/iso-22301-business-continuity/
- ISO/IEC 22313 - Business Continuity Management Systems — Guidance www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs/Managing-your-IT-and-cyber-security-incidents/Standards-for-managing-IT-security-incidents/
- Strong Password Generator. https://strongpasswordgenerator.com/

Training Statement

All staff, during induction are made aware of the organisations policies and procedures, all of which are used for training updates. All policies and procedures are reviewed and amended where necessary and staff are made aware of any changes. Observations are undertaken to check skills and competencies. Various methods of training are used including one to one, on-line, workbook, group meetings, individual supervisions and external courses are sourced as required.