CYBER SECURITY

Scope

- **Policy Statement**
- **The Policy**
- Process Requirements
- Physical Security
- Authorisation/Password Processes
- 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 including service users, residents, staff, records written or electronic, and all other corporate information, from all potentially damaging threats, internal or external, deliberate or accidental, imagined or real. Until the advent of the internet, cyber was used in the information of words relating to computers, computer networks, or virtual reality. From the Wall Street Journal to Doctor Who cyber has developed into the English language where it is currently associated with the Internet and other developing technologies. Mass cyber-attacks are almost always via Internet providers' data systems which are hacked and often the data is leaked into the mainstream media outlets. Governments now issue lots of guidance regarding cyber breaches of data protection laws and this policy reflects much of the guidance.

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, 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, of the organisation's information or data.

There are 3 elements to the process:

- Maintain the confidentiality of personal information including customers 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 the availability of the organisations information systems and services, including putting in place contingency measures that ensure 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, and 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 is in place. All staff must wear I.D. badges; individuals not doing so, in non-public areas should be challenged.

- Visitors must sign in and be accompanied at all times.
- 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 etc and checked accordingly.
- To prevent a malware contamination, no external hardware such as USB, Memory, or Recording Portable devices can be used within the organisations, without prior approval from the Director.
- Management of computers and/or networks is controlled via a contractual arrangement with our in-house IT. team.
- Users, shall not install software, for any purpose, unless authorised to do so by the Director.
- Users 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 never be shared and changed at regular intervals.
- Disposal of equipment is allowed only by authorised personnel.
- Secure transfer of files and documentation whether physically or electronically, must be properly recorded and approved.
- 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.
- Adequate and appropriate monitoring of the information that is held and its use, should be undertaken at least annually, as part of the audit cycle.
- Records 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 removed or covered when left unattended on desks or work surfaces.
- 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.

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 are regularly available and accessible to staff.
- All breaches of information security, actual or suspected are recorded, reported, and investigated, and mitigating measures are put into place to prevent a re-occurrence.

Authorisation/Password Processes

Process for Administrator Approval

All employees that are given access to the company's internal data/information systems, must be approved by a Senior Member of the Management team. The person responsible for authorising and signing off new applications is the Department head.

Access is granted/activated by our internal IT management, no other person or agency is authorised to complete this process.

New Employees

When adding new or existing employees, the Director (Amend as necessary) will complete the form of a new starter which includes the access rights granted and send it via email to the authorised IT Contractors/person, who will confirm receipt by return.

The Authorised IT contractor/Person will add the employee details and their access rights to the company's internal information systems. An email will be sent to the Authorising Director confirming that the new employee and their access rights have been added to the system.

The Director Hitendra Sharma will add the new employee's details to a central register of employee access rights.

The Director will confirm via email that the employee has been added to the Central Register to confirm and finalise the authorisation process. This will invoke the Authorised IT contractor/person to activate the account/s.

Employees Leaving

When employees leave, on the day the resignation or dismissal is confirmed, the Director will complete a leavers form (add ref) which includes the access rights that must be deleted**. This will include the date of leaving and it will be sent via email to the authorised IT person who will confirm receipt by return.

** *In some circumstances it may be necessary to remove certain access rights before the employee leaves the company such as sensitive commercial information*

The Authorised IT contractor/person will schedule the removal of access rights on the day the employee leaves the company unless otherwise stated. An email will be sent to the Authorising Director confirming that the employee and their access rights have been scheduled to be removed from the system.

At the end of the business day, the employee leaves the company. The Authorised IT person will delete the employee that the employee and their access rights have been removed from the system.

The Director will then remove the employee from the system.

The document will be controlled with version numbers to ensure the correct and most up-to-date version is used.

Review of Administrator Access (**Amend/Delete to insert your process**)

Administrator Access will be reviewed by the Director periodically or as circumstances demand.

Any changes (for example if an employee's role or responsibilities change) needed will be amended on the central register by:

- Access Rights to be removed – Highlighted in Red
- Access Rights to be added – Highlighted in Green
- The date will be amended for each employee to highlight the effective date of the changes
- The Version Control Section will be completed on the Central Register

The amended Central Register will be sent to the Authorised IT contractor/person via email who will confirm receipt by return via email

The Authorised IT Contractor/person will amend the Access Rights on the internal system using the information provided on the Central Register

The amended register will be saved with a new version number and recorded on the version control record.

Password Security

Robust Password security is essential to protect against cyber-attacks.

When access is granted, a temporary password is generated for the employee to log on to the system for the first time.

This organisation adopts the NCSC's three random words approach which combines three random words to create a password that's "long enough and strong enough".

A good way to make a password difficult to crack is by combining three random words to create a single password (for example *mondaychairgrass23*). Or use a password manager (if available), which can create strong passwords (and remember them).

For additional security, the use of gaps or hyphens should be used (for example *mon-day chair-grass 23).*

Avoid the most common passwords that criminals can easily guess (like ‘password’). Avoid creating passwords from significant dates (like birthdays), favourite sports teams, or by using family and pet names. Most of these details can be found within a person’s social media profile.

If thinking of changing certain characters in the password (so swapping the letter ‘o' with a zero, for example), cybercriminals know these tricks as well. So, the password will not be significantly stronger, but it *will* be harder to remember.

Passwords must be changed quarterly, unless otherwise requested to do so by the Director.

Employees should put a reminder in their electronic diaries to remind them to change their passwords regularly.

Passwords must never be shared with anyone both outside and inside the organisation.

New User Accounts

Administrators have the authority to raise requests to add and remove users from the system. Users are employees that require access to certain systems or data to carry out their duties effectively such as care managers, care workers, or care administrators.

Process

The administrator will send a new user request form to the Director for approval via email. The form will detail which system of systems the user will have access to, and the date access is to commence.

If the Director approves the request, the form will be returned to the administrator via email.

The approved New User Request Form will then be sent to the Authorised IT person and the user will be added to the system. An email will be sent to the Administrator confirming the user has been added

The Administrator will then add the new user to a Version Central Users record and save the document with the new version number.

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, an investigation with a report, in a timescale appropriate to the risks to the business, will be completed by the Director.
- 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 l**ikelihood** of such a threat occurring.

To mitigate risks, we will work towards a “paper lite” environment as outlined in our business plan.

Information Sharing Guidance

This clarifies information sharing for staff at all levels of the organisation. Where staff is in any doubt as to whether it is appropriate to share information, advice should be sought from the data controller.

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 must 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 about adults at risk is:

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

It is a 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 and external contacts, and any request for such information will only be shared when all the Golden Rules are met.

The Golden Rules

- Remember that the UK data protection act 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 the 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, and 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 well-being: base your information-sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
- Adhere to all policies regarding transporting confidential and sensitive information including staff records.

Related Policies

Confidentiality

Co-operating with other Providers

Data Protection Legislative Framework (UK GDPR)

Internet Email and Mobile Phone

Record Keeping

Social Media and Networking

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/

NHS Digital:
www.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
https://www.iso.org/standard/75652.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 organisation's policies and procedures, all of which are used for training updates. All policies and procedures are reviewed and amended where necessary and staff is made aware of any changes. Observations are undertaken to check skills and competencies. Various methods of training are used including one-to-one, online, workbook, group meetings, individual supervisions, and external courses sourced as required.

Date Reviewed: March 2024

Person responsible for updating this policy: Hitendra Sharma

Next Review Date: March 2025