Data Protection Policy and Procedure.

Purpose

This policy will highlight how Style Acre complies with the Data Security and Protection (DSP) Toolkit. This enhances our suite of Policies that cover Data Protection, Cyber Security and general UK GDPR compliance. As well as providing a social care perspective for Style Acre on information governance, it will provide best practice principles through the Data Security and Protection Toolkit (DSPT) in order to demonstrate what needs to be part of Style Acre culture in order to continue to receive NHS contracts. This policy also covers how we prevent data security breaches and how we react to them when prevention is not possible. A breach can either be purposeful or accidental.

To support Style Acre in meeting the following Key Lines of Enquiry:

Key Question	Key Lines of Enquiry
WELL-LED	W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?
WELL-LED	W5: How does the service work in partnership with other agencies?

To meet the legal requirements of the regulated activities that {Style Acre} is registered to provide:

- The Care Act 2014
- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Data Protection Act 2018
- UK GDPR

Policy

Style Acre will adhere to the following Principles

1. We will be open and transparent with the people we support and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012.
2. We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

3. We will establish and maintain policies for the controlled and appropriate sharing of the people we support and employ's information with other agencies, taking account all relevant legislation and citizen consent.

4. Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in our Record Keeping Policy. We ensure that it is as easy to withdraw as to give consent.

5. We will undertake annual audits of our compliance with legal requirements.

6. We acknowledge our accountability in ensuring that personal data shall be:
   - Processed lawfully, fairly and in a transparent manner;
   - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
   - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
   - Accurate and kept up to date;
   - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
   - Processed in a manner that ensures appropriate security of the personal data.

7. We uphold the personal data rights outlined in the GDPR;
   - The right to be informed;
   - The right of access;
   - The right to rectification;
   - The right to erasure;
   - The right to restrict processing;
   - The right to data portability;
   - The right to object;
   - Rights in relation to automated decision making and profiling.

Due to our size, we have determined that we are not required to have a Data Protection Officer (DPO), as we do not process special categories of data on a large scale. Nonetheless, to ensure that every individual's data rights are respected and that there are the highest levels of data security and protection in our organisation, we have appointed a member of staff to be our Data Security and Protection Lead. The Data Security and Protection Lead will report to the highest management level of the organisation. We will support the Data Security and Protection Lead with the necessary resources to carry out their tasks and ensure that they can maintain expertise.

We complete the Data Security and Protection Toolkit on an annual basis and our publication status can be found here:
https://www.dsptoolkit.nhs.uk/OrganisationSearch

Underpinning policies & procedures

This policy is underpinned by the following:

1.7.1. Record Keeping Policy – details transparency procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures), information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share;

1.7.2. Network Security Policy – outlines procedures for securing our network;

1.7.3. Business Continuity Plan –outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day to day running of our organisation;

1.7.4. Staff Code of Conduct - provides staff with clear guidance on the disclosure of personal information.

2. Data protection by design & by default

1. We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

2. We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

3. All new systems used for data processing will have data protection built in from the beginning of the system change.
4. All existing data processing has been recorded on our Record of Processing Activities (ROPA). Each process has been risk assessed and is reviewed annually.
5. We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.
6. In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.
7. Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

3. Responsibilities

1. Our designated Data Security and Protection Lead is Rebecca Speight. The key responsibilities of the lead are:
    - To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles;
    - To define our data protection policy and procedures and all related policies, procedures and processes and to ensure that sufficient resources are provided to support the policy requirements.
    - To complete the Data Security & Protection Toolkit (DSPT) annually and to maintain compliance with the DSPT.
    - To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with senior management.

4. Data Security

This Data Security Policy covers:

- Physical Access procedures;
- Digital Access procedures;
- Access Monitoring procedures;
- Data Security Audit procedures;
- Data Security Breach procedures.

4.1 Physical Access Procedures

Physical access to records shall only be granted on a strict 'Need to Know' basis.

During their induction each staff member who requires access to confidential information for their job role will be trained on the safe handling of all information and will be taught the procedures which govern how data is used, stored, shared and organised in our organisation.

Our staff must retain personal and confidential data securely in locked storage when not in use and keys should not be left in the barrels of filing cabinets and doors.

The Information Asset Register (IAR) will contain the location of all confidential and sensitive personal information.

We will risk assess each storage location to ensure that the data is properly secured. This risk assessment forms part of the IAR.

4.2 Digital Access Procedures

Access shall be granted using the principle of 'Least Privilege'. This means that every program and every user of the system should operate using the least set of privileges necessary to complete their job.

We will ensure that each user is identified by a unique user ID so that users can be linked to and made responsible for their actions.

The use of group IDs is only permitted where they are essential for the work carried out.

A record is kept of all users given access to the system. This record is held by the IT Manager.

In the instance that there are changes to user access requirements, these can only be authorised by the Data Security and Protection Lead or equivalent job role.

The IAR will contain the location of all confidential and sensitive personal information which is digitally stored.

We will follow robust password management procedures and ensure that all staff are trained in password management.

As soon as an employee leaves, all their system logons are revoked.

The Data Security and Protection Lead or equivalent job role will review all access rights on a regular basis, but in any event at least once a year. The review is designed to positively confirm all system users. Any lapsed or unwanted logons which are identified are disabled immediately and deleted unless positively reconfirmed.

When not in use all screens will be locked and a clear screen policy will be followed.

4.3 Access Monitoring Procedures

The management of digital access rights is subject to regular compliance checks to ensure that these procedures are being followed and that staff are complying with their duty to use their access rights in an appropriate manner.

Areas considered in the compliance check include whether:

- Allocation of administrator rights is restricted;
- Access rights are regularly reviewed;
- Whether there is any evidence of staff sharing their access rights; staff should know that this can result in disciplinary action;
- Staff are appropriately logging out of the system;
- Our password policy is being followed;
- Staff understand how to report any security breaches.

4.4 Data Security Audit Procedures

Confidentiality audits will focus on controls within electronic records management systems and paper record systems; the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems,

or as a result of insufficient controls. Audits of security and access arrangements within each area are to be conducted on a six-monthly rolling programme. How frequently you audit information can vary, but as a minimum there should be a full annual audit.

Audits will be carried out as required by some or all of these methods:

1. Unannounced spot checks to random work areas;
2. Based on electronic reports from care planning software or auditing of care plans. This can be from your ICT contractor or from internal monitoring.

The following checks will be made during GDPR audits which audit both security and quality.

- A review of all personal data held at Style Acre and confirmation that the data held is accurate, adequate and not excessive
- An analysis of how the data is used, and a justification for the collection and holding of the data
- An action plan to address any concerns or shortfalls in the quality of the data held at Style Acre
- A review of historical data held at Style Acre to ensure that it is all meeting current retention schedules, and where data is no longer needed, it is destroyed in line with data protection requirements
- The Information Asset Register has been reviewed, updated and signed off;
- The Record of Processing Activities has been reviewed, updated and signed off;
- A review of any breaches or failed attempts to access any confidential information.
- understanding of their responsibilities with regard to confidentiality;
- Appropriate use of workplaces, filing systems and equipment

4.5 Data Security Breach Procedures

In order to mitigate the risks of a security breach we will:

1. Follow the Physical Access, Digital Access, Access Monitoring and Data Security Procedures;
2. Ensure our staff are trained to recognise a potential data breach whether it is a confidentiality, integrity or availability breach;
3. Ensure our staff understand the procedures to follow and how to escalate a security incident to the correct person in order to determine if a breach has taken place.

In the instance that it appears that a data security breach has taken place:

1. The staff member who notices the breach, or potential breach, will complete a Data Security Breach Incident Report Form, appendix one DATA BREACH REPORTING FORM, without delay;
2. This form will be completed and handed to the Data Security and Protection Lead or equivalent job role or, if they are not available, to a member of senior management;
3. The Data Security and Protection Lead will complete the rest of the Incident Report Form and conduct a thorough investigation into the breach;
4. In the instance that the breach is a personal data breach and it is likely that there will be a risk to the rights and freedoms of an individual then the Information Commissioner's Office (ICO) will be informed as soon as possible, but at least within 72 hours of our discovery of the breach.

5. Responsibilities

Rebecca Speight is responsible for physical security;

Rebecca Speight is responsible for updating and auditing the IAR and ROPA;

Keith Thornton is responsible for digital access;

Chris Ingram is responsible for managing breaches;

Sarah Stuart is responsible for data security audits.

6. Approval

This policy has been approved by the undersigned and will be reviewed at least annually.

Style Acre
Supporting people with learning disabilities

OFFICE USE Date: Initials: Record Number:

DATA BREACH REPORTING FORM

MUST BE REPORTED TO THE DATA PROTECTION OFFICER WITHIN 24 HOURS OF THE DATA BREACH

Date:		Time:	

Name of support manager/on call contacted:	
Date and time contacted:	
Name of person recording the data breach:	
Name of person(s) involved in the data breach:	
Location of data breach:	
Data subjects affected by breach:	
Amount of data compromised during data breach:	
Type of data compromised during breach:	

Record of events (*Please use a separate sheet of paper if needed)*

Actions Taken to address the breach & mitigate possible side effects:

1)
2)
3)

Staff Signature:	**Date:**

Office Use:

Chief Executive Notified of Breach:	
Why:	
Data breach reported to ICO within 72 hours of occurring:	
Why:	

Was the breach avoidable?

If so how:

Actions taken by Data Protection Officer following breach:

Data Protection Officer Signature:	Date: