**INFORMATION GOVERNANCE POLICY**

# Purpose

This policy is important because it will help the Zenith Care Recruitment staff to understand how to look after the information, they need to do their jobs, and to protect this information on behalf of service users.

Information is a vital asset. It plays a key part in ensuring the efficient management of our service planning, resources and performance management. It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

Information Governance looks at the way the Zenith Care Recruitment handles service users information and staff, with particular consideration of personal and confidential information. Without access to information, it would be impossible to provide quality care and good corporate governance. A robust governance framework needs to be in place to manage this vital asset, providing a consistent way to deal with the many different information handling requirements including:

* + Information Governance Management
  + Confidentiality and Data Protection Legislation assurance

The aims of this policy is to maximise the value of practical assets by ensuring that information is:

* + Held securely and confidentially
  + Obtained fairly and efficiently
  + Recorded accurately and reliably
  + Used effectively and ethically
  + Shared appropriately and lawfully

To protect the Zenith Care Recruitment’s information assets from all threats, whether internal or external, deliberate or accidental, the **Zenith Care Recruitment** will ensure that:

* + Information will be protected against unauthorised access
  + Confidentiality of information will be assured
  + Integrity of information will be maintained
  + Information will be supported by the highest quality data
  + Regulatory and legislative requirements will be met
  + Business continuity plans will be produced, maintained and tested
  + Information security training will be available to all staff

# Scope

The scope of this Policy covers all Zenith Care Recruitment service users and staff.

The Zenith Care Recruitment recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Zenith Care Recruitment fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard information. Zenith Care Recruitment also recognises the need to share information in a controlled manner. Zenith Care Recruitment believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such, it is the responsibility of Service manager and staff to ensure and promote the quality of information and to actively use information in decision making processes.

## Definitions

In order to assist staff with understanding their responsibilities under this policy, the following types of information and their definitions are applicable in all relevant policies and documents.

|  |  |
| --- | --- |
| **Personal Data** (derived from the GDPR) | Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online  identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person |
| **‘Special Categories’ of Personal Data** (derived from the GDPR) | ‘Special Categories’ of Personal Data is different from Personal Data and  consists of information relating to:   1. The racial or ethnic origin of the data subject 2. Their political opinions 3. Their religious beliefs or other beliefs of a similar nature 4. Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 5. Genetic data 6. Biometric data for the purpose of uniquely identifying a natural person 7. Their physical or mental health or condition 8. Their sexual life |
| **Personal Confidential Data** | Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal  information about identified or identifiable individuals, which should be |

|  |  |
| --- | --- |
|  | kept private or secret. The definition includes dead as well as living people and ‘confidential’ includes information ‘given in confidence’ and ‘that which is owed a duty of confidence’. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March  2013). |
| **Commercially confidential Information** | Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to Zenith Care Recruitment or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information  Regulations. |
| **Sensitive Data (Derived from GDPR)** | ‘Sensitive Data’ Data is different from Personal or Special Category data as it is derived from Article 10 of the GDPR and is information relating to “data relating to criminal convictions and offences or related security measures” |

# Legal Compliance

Zenith Care Recruitment will maintain policies to ensure compliance with Data Protection Legislation. This includes the General Data Protection Regulation (GDPR), the Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time.

In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality, the processing and sharing of personal data including the Human Rights Act 1998, the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations.

# Roles and Responsibilities

Zenith Care Recruitment has a responsibility for ensuring that it meets its corporate and legal responsibilities and for the adoption of internal and external governance requirements. Zenith Care Recruitment is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

## Management Team

It is the role of the service manager to define Zenith Care Recruitment policy in respect of Information Governance, taking into account legislative and care quality commission requirements.

The Service Manager is also responsible for:

* + ensuring that sufficient resources are provided to support the requirements of the policy
  + appropriate mechanisms are in place to support service delivery and continuity

The Service Manager is also responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance; coordinating Information Governance in Zenith Care Recruitment and raising awareness of Information Governance.

All staff have responsibility for complying with this policy and with Data Protection Legislation; the following roles have specific responsibilities:

## Data Protection Officer

The Data Protection Officer (DPO) is the person that has been identified within Zenith Care Recruitment that has the responsibilities as set out in the GDPR guidance. This includes monitoring compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments, giving due regard to the risks associated with the processing of data undertaken by Zenith Care Recruitment and acting as the contact point with the ICO.

# Processes/Requirements

Zenith Care Recruitment will ensure that it meets its national requirements in respect of its submission of the annual self-assessment Data Security and Protection Toolkit (DSPT).

Non-confidential information about Zenith Care Recruitment and its services will be available to the public through a variety of media.

Zenith Care Recruitmentwill maintain policies to ensure compliance with the Freedom of Information Act. Zenith Care Recruitment will maintain clear procedures and arrangements for handling requests for information. Zenith Care Recruitment will maintain policies to ensure compliance with the Records Management Code of Practice for Health and Social Care (2016).

# Information Security

Zenith Care Recruitment will maintain policies for the effective and secure management of its information assets and resources.

Zenith Care Recruitment will promote effective confidentiality and security practice to its staff through policies, procedures and training.

Zenith Care Recruitment will adhere to the Digital Guide to the Notification of Data Security and Protection Incidents and as part of this, will review and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches. Under Data Protection Legislation, where an incident is likely to result in a risk to the rights and freedoms of the Data Subject/individuals the Information Commissioner’s Office (ICO) must be informed no later than 72 hours after Zenith Care Recruitment becomes aware of the incident. Please refer to Zenith Care Recruitment Incident Reporting Policy.

# Information Quality Assurance

Zenith Care Recruitment will maintain policies and procedures for information quality assurance and the effective management of records.

Zenith Care Recruitment will undertake or commission annual assessments and audits of its information quality and records management arrangements. Staff are expected to take ownership of, and seek to improve, the quality of information within Zenith Care Recruitment. Wherever possible, information quality should be assured at the point of collection.

Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

# Implementing new services

The Data Protection Officer should be consulted during the design phase of any new service, process or information asset and contribute to the statutory Data Protection Impact Assessment (DPIA) process when new processing of personal data or special categories of personal data is being considered. Responsibilities and procedures for the management and operation of all information assets should be defined and agreed by the management of Zenith Care Recruitment.

# Training

All Zenith Care Recruitment new staff must undertake Data Security induction training via an approved training platform to evidence compliance with the Data Protection Legislation as part of the induction process. Extra training will be given to those dealing with requests for information. A register will be maintained of all staff who have completed the annual data security online training.

# Monitoring and Review

This policy will be monitored by Service Manager to ensure any legislative changes that occur before the review date are incorporated.

Compliance with Zenith Care Recruitment policies is stipulated in staff contracts of employment. If staff members are unable to follow Zenith Care Recruitment policies or the policy requirements cannot be applied in a specific set of circumstances, this must be immediately reported to the Line Manager, who should take appropriate action. Any non-compliance with Zenith Care Recruitment policies or failure to report non-compliance may be treated as a disciplinary offence.

This policy will be reviewed Annually by the Registered Manager, or sooner if required by law.

|  |  |
| --- | --- |
| Signed: | \_\_\_\_\_\_\_Kechi Anyanwu\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Date: | \_\_\_\_\_\_05th November 2021\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |
| Policy review date: | \_\_\_\_\_20th April 2022\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |