**Data Protection Policy**

The Data Protection Act 1998 gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The purpose of this policy is to enable **sedcat** to:-

* Comply with the law in respect of the data it holds about individuals;
* Follow good practice;
* Protect **sedcat** users, staff, Trustees, volunteers and other individuals
* Protect the Organisation from the consequences of a breach of its responsibilities

**The Data Protection Act 1998**

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

Anyone who processes personal information must comply with 8 principles which make sure that personal information is :

* Fairly and lawfully processed
* Processed for limited purposes
* Adequate, relevant and not excessive
* Accurate and up to date
* Not kept for longer than is necessary
* Processed in line with the rights of Data subjects
* Secure
* Not transferred to other countries without adequate protection.

The second area covered by the act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

The Information Commissioner’s Office (ICO) is the Regulator of the Act and:-

* registers and holds information on, data controllers.
* Handles concerns and complaints
* Takes enforcement action and can issue fines and criminal prosecution against organisations and individuals

**sedcat** is the Data Controller and is registered under the Data protection Act 1998. All processing of personal data will be undertaken in accordance with the data protection principles.

The Board of Trustees recognises its overall responsibility for ensuring that **sedcat** complies with its legal obligations.

The Data Protection Officer at **sedcat** is the **sedcat Chief Officer** and is the central point of contact for all data compliance issues.

**sedcat Policy statement**

 **sedcat** will:

* Comply with both the law and good practice
* Respect individuals rights
* Be open and honest with individuals whose data is held
* Provide training and support for staff and volunteers who handle personal data, so they can act confidently and consistently.

**sedcat** recognises that its first priority under the Data Protection Act is to avoid causing harm to individual. Information about staff, volunteers and users will be used fairly, securely and not disclosed to any person unlawfully.

The Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, **sedcat** will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

Each member of staff and volunteer at sedcat who handles personal data will comply with **sedcat** operational procedures for handling personal data to ensure that good Data Protection practice is established and followed.

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy will be handled under **sedcat** disciplinary procedures.

Because confidentiality applies to a much wider range of information than Data protection, **sedcat** has a separate Confidentiality Policy. This Data Protection policy should be read in conjunction with **sedcat** Confidentiality Policy,

In order to provide some services, sedcat may need to share client’s personal data with other agencies (Third parties). Verbal or written agreement will always be sought from the client before data is shared.

Where anyone within **sedcat** feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done after discussions with the Data Protection officer. All such disclosures will be documented.

**Security**

This section of the Policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any aspect of security.

Any recorded information on users, volunteers and staff will be ;

* Kept in locked cabinets
* Protected by the use of passwords if kept on computer
* Destroyed confidentially if it is no longer needed.

Staff and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is displayed.

Where service users have access to the office whilst employees are working, privacy screens should be used to shield information or service users should be restricted to certain parts of the office space where employees are not working.

Service users should be kept as far away from office working space as possible to avoid overhearing telephone conversations.

* Notes regarding personal data of users should be shredded or destroyed
* Driver schedules must be handled with care and kept away from passengers during travelling and shredded upon return to the office.

*Policy last review: 31/10/2023*