Choices and Voices

Data Protection Policy

Introduction

Choices and Voices is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all our legal obligations.
We may at times hold personal data about our employees, clients, suppliers, and other individuals **for a variety of business purposes.**

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. This policy requires staff to ensure that the Data Protection Manager (DPM) is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. *Business purposes include the following:* *- Compliance with our legal, regulatory, and corporate governance obligations and good practice* *- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* *- Ensuring business policies are adhered to (such as policies covering email and internet use)* *- Operational reasons, such as recording transactions, training, and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking* *- Investigating complaints* *- Checking references, ensuring safe working practices, monitoring, and managing staff access to systems and*

	facilities and staff absences, administration, and assessments *- Monitoring staff conduct, disciplinary matters* *- Marketing our business* *- Improving services*
Personal data	'Personal data' means 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. *Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	'Data controller' means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and

	means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office.

Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms.
This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?
As our Data Protection Manager (DPM), Michelle Sanderson has overall responsibility for the day-to-day implementation of this policy. You should contact the DPM for further information about this policy if necessary.

Michelle Sanderson info@choicesandvoices.org.uk

Section 1.
The principles

Choices and Voices shall comply with the principles of data protection (the principles) enumerated in the UK General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The principles are:

Lawful, fair, and transparent
Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

Limited for its purpose
Data can only be collected for a specific purpose.

Data minimisation
Any data collected must be necessary and not excessive for its purpose.

Accurate
The data we hold must be accurate and kept up to date.

Retention
We cannot store any data longer than 12 months on completing work for local authorities or Trusts via our secure cloud-based system.
Personal data regarding staff will be held for 12 months on completion of work for Choices and Voices.

Integrity and confidentiality
The data we hold will be kept safe and secure via our secure cloud-based system. All data in terms of what is stored within the UK, including the Office 365 backup SaaS platform, which is stored in the UK.
We are registered with the ICO and a have an accredited Cyber Essentials Certification.

Accountability and transparency

We ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the DPM.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. All staff are responsible for understanding their responsibilities and will receive regular updates and training to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Complement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security and enhanced privacy procedures on an ongoing basis

Section 2

Choices and Voices Commitment

The ICO is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about customers, staff or those who work or interact with us.

- **Information Asset Owners** – we assign an Information Asset Owner (IAO) to each information asset throughout the organisation, who together with a network of teams and staff with information management responsibilities aid the ICO in managing personal data and its associated risks.
- **Privacy Notices** - we publish a privacy notice on Choices and Voices website and provide timely notices where this is required. We track and make available any changes in our privacy notice. We also publish a staff privacy notice and keep it up to date.
- **Training** - we require all staff to undertake mandatory training on information governance and security which they re-take every year. In addition, all staff are required to attend a more detailed data protection training module as part of their induction.

- **Breaches** - we consider personal data breach incidents and have a reporting mechanism that is communicated to all staff. We assess whether we need to report breaches to the ICO as the Regulator of DPA. We take appropriate action to make data subjects aware if needed.
- **Information Rights** - we have a and clear processes to handle subject access requests and other information rights requests.
- **Data Protection by Design and Default** - we have a procedure to assess processing of personal data perceived to be high risk, that needs a Data Protection Impact Assessment (DPIA) carried out, and processes to assist staff in ensuring compliance and privacy by design is integral part to any product, project or service we offer.
- **Records of Processing Activities (ROPAs)** - we record our processing activities and publish our safeguards policy on processing of data.
- **Policies and Procedures** - we produce policies and guidance on information management and compliance that we communicate to staff.
- **Communications** - We have a clear communication plan which seeks to embed a culture of privacy and risk orientation.
- **Contracts** - Our Commercial department oversee that our contracts are compliant with UK GDPR.

Section 3.
Fair and lawful processing

We process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this

happening. If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

Controlling vs. processing data

Choices and Voices is classified as a data controller and processor. We maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling data.