Data Management Policy

1. Context and overview

Introduction:

Diversity Voice needs to gather and use certain information about individuals.This can include the general public, service users, contractors, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

Why this policy exists:

This data management policy ensures Diversity Voice:

- Complies with data protection law and follows good practice
- Protects the rights of individuals, staff and partners
- Is transparent about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law:

The General Data Protection Regulation (GDPR) applies in the UK and across the EU from May 2018. It requires personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5. 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; personal data may be stored for longer periods insofar as the personal data will processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals

6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Diversity Voice acknowledges that its Board of Directors holds overall responsibility for compliance with these principles, and responsibility for the ability to demonstrate compliance. The day-to-day responsibility of compliance will rest with the employees.

This policy is intended to work in conjunction with Diversity Voice Safeguarding Policy and Procedures, Equality & Diversity Policy and Health & Safety Policy.

2. Definitions

For the purposes of this policy the term 'employee' will refer to anyone we work with: anyone employed by Diversity Voice, anyone engaged as a freelancer or working as a volunteer (including directors). The term 'applicant' will refer to anyone applying for any of the above types of roles with the company.

Legal Definitions of the General Data Protection Regulation (GDPR) 2018:

Personal Data

Any information relating to an identifiable person, for example: name, postal address, email address, telephone number, banking details and social media account names or handles. This also includes online identifiers such as location data and cookies.

Special Categories of Personal Data

Sensitive personal data. For example, data that reveals an individual's racial or ethnic origin, or sexual orientation.

A Data subject

Someone whose personal data is processed.

A Data controller

The organisation who determines the purposes for which and the manner in which any personal data is processed. In this case, Diversity Voice.

A Data processor

Any person (other than an employee of the data controller) who processes the data on behalf of the data controller

3. People and responsibilities

Everyone at Diversity Voice contributes to compliance with GDPR.

Action	Responsibility
Keeping directors updated about data protection issues, risks and responsibilities	Chief Executive
Documenting, maintaining and developing the organisation's data protection policy and related procedures, in line with agreed schedule	Operations Manager
Embedding ongoing privacy measures into organisation's policies and day-to-day activities, throughout the organisation. The policies themselves will stand as proof of compliance.	Chief Executive and Operations Manager
Dissemination of policy across the organisation, and arranging training and advice for staff	Operations Manager
Dealing with subject access requests, deletion requests and queries from clients, stakeholders and data subjects about data protection related matters	Operations Manager
Checking and approving contracts or agreements with third parties, (if in place) that may handle the organisation's sensitive data	Operations Manager and Chief Executive
Ensuring all systems, services and equipment used for storing data meet acceptable security standards	Operations Manager
Performing regular checks and scans to ensure security hardware and software is functioning properly	Operations Manager and staff members
Evaluating any third party services the organisation is considering using to store or process data, to ensure their compliance with obligations under the regulations	Operations Manager
Developing privacy notices to reflect lawful basis for fair processing, ensuring that intended uses are clearly articulated, and that data subjects understand how they can give or withdraw consent, or else otherwise exercise their rights in relation to the 0rganisations use of their data	Operations Manager
Ensuring that audience development, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the GDPR principles	Chief Executive

Data Protection Officer (DPO)– the person responsible for fulfilling the tasks of the DPO in respect of Diversity Voice is: Operations Manager Anita Mosedale

Organisations with more than 250 employees must appoint a Data Protection Officer. This does not currently apply to Diversity Voice.
However, regardless of whether the GDPR obliges you to appoint a DPO, we must ensure that the organisation has sufficient staff and skills to discharge your obligations under the GDPR. Best practice dictates that, irrespective circumstances, organisations should appoint a named individual as DPO to lead on ensuring that data protection obligations are met. The minimum tasks of the DPO are:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits

To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.)

4. Scope of personal information to be processed

We ask for your data so that we can:

- provide our services
- keep you up to date with information about our work; and
- inform you of the ways that you can get involved with or support the organisation.

The type of information we will collect about you may include:

1. your name
2. your postal address
3. your telephone numbers
4. your email address
5. ethnic origin
6. country of origin
7. date of birth
8. gender
9. education information
10. native language

If you pay for a service, we will also process data as part of that financial transaction.

We will never collect sensitive information about you without your explicit consent.

Your data will only be disclosed to third parties in order to provide these services to you. Your personal information will not be passed to third parties for marketing purposes, unless you have given specific consent.

Where the data is collected from and stored
Appropriate security measures must be in place for hard copy records and files being kept in locked cupboards, as well as for digital data. Digital data is kept on a secure server which is only accessible to Diversity Voice employees via password and access to data may vary according to necessity, with each employee assigned a unique log-in profile with individual permissions.

How we process the data

Information about privacy policies and cookies can be found on our website.

Where individuals sign up to our mailing list, or apply for a service via a hard copy form, they will be advised where this statement can be found online. Hard copy forms will always include tick-boxes for consent and relevant short statements indicating how their personal information will be used.

Data Retention

Personal data used for the purpose of keeping you up to date, will generally be retained until consent is withdrawn.

Personal data records kept for the purposes of delivering a service will be retained for five years. Data on service delivery will be anonymised after this time period unless it contains safeguarding information. Please see Diversity Voice Safeguarding Policy.

Employee and freelancer records will be retained in line with HMRC requirements.

Records of the withdrawal of consent will be kept indefinitely, and in keeping with the data minimisation and purpose limitation.

Exemptions relating to Special Categories of Personal Data

Special Categories of Personal Data and Equality & Diversity Monitoring

The GDPR prohibits the processing of data that reveals an individual's sensitive personal data, for example racial or ethnic origin, unless with the data subject's explicit consent or in exceptional circumstances. Several of these special categories are defined in UK law as protected characteristics; Diversity Voice undertakes monitoring of the protected characteristics of its applicants and employees for the purposes of evaluating the effectiveness of our work and achieving our charitable aims. All data is provided voluntarily. We obtain and record explicit consent. We report on this data anonymously. Please see Diversity Voice Equality & Diversity Policy for more information.

Special Categories of Personal Data and UK Disclosure & Barring Service checks

The GDPR allows the processing of personal data relating to criminal records by the UK's Disclosure and Barring Service (DBS) for the purposes defined in UK law relating to safeguarding. It would also allow, for example, checking the criminal records of relevant employees (for example, an accountant) for financial misconduct offences if required. Any use or storage of such data must be carried out in accordance with UK law. Please see Diversity Voice Safeguarding Policy for more information.

Personal data relating to Children and Young People

The GDPR introduces new regulations about the processing of children's data, particularly online.

Diversity Voice collects information about children in order to be able to deliver its services. Children need particular protection when collecting and processing their personal data because they may be less aware of the risks involved.

Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

If our processing is likely to result in a high risk to the rights and freedom of children then we always do a DPIA.

If a child is not competent to exercise their own data protection rights or consent to processing themselves then it will usually be in their best interests to allow an individual with parental responsibility to act on their behalf. If a child is competent then our overriding consideration will still be what is in their best interests however, in most cases it should be appropriate to let the child act for themselves.

5Diversity Voice has an obligation to think about these issues and to identify appropriate safeguards and demonstrate that we have sufficiently protected the rights and fundamental freedoms of the child and that we have prioritised their interests over our own.

Diversity Voice has implemented the following safeguards:

- Children's data is stored securely on Diversity Voice systems.
- Only authorised staff have access to children's personal and sensitive data.
- Employees, volunteers, and freelancers sign a confidentiality agreement.
- The external organisations we work with verify parental responsibility, and we ensure that children are informed of their rights.

We collect anonymised feedback and we process anonymised data relating to overall audience numbers and trends. Images of children and young people are taken, stored and used according to our Safeguarding Policy which ensures informed, positive consent from parents or carers of those under the age of 16. Please see Diversity Voice Safeguarding Policy for more information.

5. Uses and conditions for processing

Determining lawful basis for processing
Diversity Voice will only process personal data in compliance with the GDPR's standards of lawful basis. Those most relevant to Diversity Voice activities include circumstances in which:
1. Processing is necessary for the **performance of a contract** with the data subject, or to take steps to enter into a contract
2. Processing is necessary for **compliance with a legal obligation**
3. Processing is necessary for the purposes of **legitimate interests** pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.
4. The data subject gives their **consent**

Consent
In order to promote the organisation's work we collect, hold and process personal data relating to members of the public on our mailing list. Diversity Voice, as a registered charity, also collects, holds and processes personal data relating to members of the public who make donations to support our work. We will only collect, hold and process such data where individuals have given their consent for us to do so.

Consent must be:
- Unambiguous and positively affirmed
- Specific and Informed
- Freely given
- Recorded
- Possible to withdraw

Consent for employees and applicants

6Some personal data relating to applicants and employees is collected voluntarily rather than as a necessity. In such cases the same principles of consent apply.

Lawful basis for processing

Outcome/Use	Processing required	Data to be processed	Conditions for processing	Evidence for lawful basis
Event information	Name and contact details from database	Name and contact details	Consent	Opt-in
Training opportunities	Name and contact details from database	Name and contact details	Consent	Opt-in
Employment and freelance work opportunities	Applications by email	Name and contact details Personal background info	Legitimate interest	Act as employer, maintain payroll, issue assignments
Volunteer management	Applications by email Contacts from database	Name and contact details	Consent	Opt-in
Research	Form on website Telephone and f2f surveys	Name and contact details Personal info including gender, country of origin	Consent	Opt-in
Translation & Interpreting Services	Data from client meetings; translation sources	Data from client meetings, translated documents and original translations.	Consent where required for personal sensitive data, e.g. social services, and legitimate interest eg business translations	Meet contractual requirements; legitimate business interest
Education reports	Data from school reports stored on winSCP	Name, date of birth	Contract	Meet contractual requirements
Feedback forms	Data entered on website, held on portal, analysed in Excel, processed and sent without personal data	Name and contact details	Consent	Meet contractual requirements Legitimate interest
Training records	Registration form	Name, contact details, information related to background and	Consent	Opt-in

		experience for the purpose of planning training		

6. Privacy Impact Assessments

DPIA Assessment Form

- Data Protection Impact Assessments are a tool which will help identify the most effective way to comply with our data protection obligations and meet individual expectations of privacy. The attached template will be used prior to commissioning a new system, or processing a new set of personal data of changing the processing of an existing personal data set.
- An effective DPIA will organisations to identify and resolve problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.
- This DPIA is based on guidance documents provided by the information commissioner's office (ICO) to support the date protection by design approach and the information captured will ensure reasonable steps are taken during the implementation of any new system or process.
- **DPIA Screening Questions**
- **Is a DPIA mandatory?**

Mandatory DPIA Screening Question	**Yes or No**
Will the project make use of a new technology (system)?	
Will the project involve systematic and extensive processing activities,	
including profiling and where decisions that have legal effects – or similarly	
significant effects – on individuals	
Will the project involve the large scale processing of special categories of	
personal data	
Will the project involve the large scale, systematic monitoring of public	
areas (CCTV)	

- If the answer to any of the above is "Yes" it is necessary to complete a DPIA.
- **Is a DPIA best practice**

Recommend DPIA screening questions	**Yes / No**
Will the project involve the collection of new information about individuals?	
Will the project compel individuals to provide information about themselves?	
Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a purpose it is not currently being used for, or in a way it is not currently used?	
Will the project require you to contact individuals in ways that they may	

find intrusive?	

- If the answer to any of the above is “Yes” a DPIA may be recommended as best practice.
- Where it is mandatory or recommended to complete a DPIA an assessment will take place to ensure the new systems comply with the core 6 principles of GDPR.

7. Data Sharing

Third Parties

Diversity Voice will only work with third parties and/or external data processors who are also fully compliant with the 2018 GDPR and will ensure that any contract for external data processing is also fully compliant.

Current third parties include:

- Kashflow.co.uk
- Microsoft 365
- Server host: Ionos.com
- WinSCP
- nestpensions.org.uk
- Albert Goodman and Eleanor Berry: Accountant and annual audit

Where consent is the basis for sharing, Diversity Voice will obtain and necessary specific, clear, granular permissions for sharing data with NAMED third parties, for specifically defined uses, and in specified communications channels. Where other lawful conditions for processing are relied upon for data sharing, these will also be described.

Details will be given as to when data sharing agreements, describing and ensuring the arrangements concerning the collection of the necessary permissions, defining the scope of the personal data to be shared – along with the meta-data that will enable the receiving party to be able to create an audit trail, sufficient to enable them to respond to any challenge as to why an individual’s data has been processed, or to facilitate a data subject access request, and which details the security measures that will be put in place to protect the data in transit, and which establishes the shared understanding of the receiving organisations’ obligations as a data controller with responsibility for all aspects of the regulation as data controllers of the new copy of the data which is being shared with them.

8. Security Measures

The actions to reduce the risk of any data protection issues identified in section are detailed below.

Risk to individuals	Solution	Result
Leak of personal and/or special categories of personal data to an external organisation	Any data files shared will be subject to encryption/ password protection. Passwords: Strong passwords are to be used at all times for accessing systems. File sharing will be by invitation only over agreed file sharing systems and to agreed standards	Limit risk of unintended data leak or expose to data of unknown system threats
Record held/modified to include correct information	Data audits to be conducted to verify the accuracy and quality of data held.	Lower risk of inaccurate data being stored.
Unauthorised access to personal and/or	Data access controls in place to ensure access to data is set against user profiles	Lower risk of unauthorised access
Implementation of new systems: leak of personal data/inaccurate data being transferred to new systems	DPIA assessment to be carried out	Assess and lower any identified areas of risk prior to project being started
Lack of internal understanding of GDPR requirements	Training to be provided for all employees	Lower risk of breach and ensure compliance

In addition to the above the following will be undertaken

Reviewing of security measures: The GDPR security measures will be assessed annually to understand the ongoing risks faced by the organisation

Assessing if a personal data protection breach has occurred:

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. An assessment will be made against the ICOs guidance to determine if a data breach has occurred.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Reporting a breach

If it is determined a breach has occurred, it will be reported to the ICO in accordance with ICO regulations. The reporting of any breaches will be in line with the current ICO regulations: Full details

are found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

9. Subject access requests

All individuals who are the subject of data held by the organisation are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

Process for managing Data Subject Access requests

1. All requests should be made in writing (which includes email) and addressed to Diversity Voice. Once the request has been received Diversity Voice will contact the data subject to confirm receipt. At this point Diversity Voice will have 30 days from receipt of the request in which to process the request

2. Once the information has been gathered and is ready to be handed over to the data subject, Diversity Voice will contact the data subject to make arrangements for its collection or delivery

3. Prior to handing over personal data, Diversity Voice will need to confirm the identity of the data subject.

10. The right to be forgotten

Managing requests for erasure:

All requests for erasure will be managed on a case by case basis. However, Diversity Voice will:

1. Verify the identity of the individual making the request
2. Explain the implications of full erasure
3. Conduct a full audit of data held (including 3rd parties) and assess erasure as appropriate
4. Notify the individuals once the process has been completed

11. Privacy notices

Diversity Voice aims to ensure that individuals are aware that their data is being processed, and that they understand:

- Who is processing their data
- What data is involved
- The purpose for processing that data
- The outcomes of data processing

- How to exercise their rights.

To these ends the organisation has relevant privacy statements, setting out how data relating to these individuals is used by the company.

A privacy statement covers the members of the public that can be viewed by individuals via our website, and anyone signing up to our mailing list, and they are directed to it before they provide their personal information and their consent.

12. Ongoing documentation of measures to ensure compliance

Meeting the obligations of the GDPR to ensure compliance will be an ongoing process. Diversity Voice details here the ongoing measures implemented to:

1) Maintain documentation/evidence of the privacy measures implemented and records of compliance
2) Regularly test the privacy measures implemented and maintain records of the testing and outcomes.
3) Use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts.
4) Keep records showing training of employees on privacy and data protection matters.

Appendix

Data Assessment

Type of data	Description	Where stored	Purpose	Usage restriction	Retention period
Client information; individuals seeking advice, training course participants	Personal and sensitive data including names, contacts, ethnic original, date of birth, gender, education background, age, native language, nationality	Microsoft 365	Delivering services	Only available to staff who need access for the purpose of their duties; differentiated permissions	Up to 5 years
Employee, volunteer and freelancer information	Personal information including name, contacts.	Microsoft 365 Ionos.com Kashflow.co.uk Nestpensions.co.uk Lockable cabinet	Act as employer, maintain payroll, pension, manage work assignments	Only available to staff who need access for the purpose of their duties; differentiated permissions	Up to 5 years
Personal and sensitive data of children	Personal and sensitive data including names, contacts, ethnic original, date of birth, gender, education background, age, native language, nationality and education information	Microsoft 365 with secure Egress mail	Provide contract services	Only available to staff who need access for the purpose of their duties; differentiated permissions	Up to 3 months
Research data	Personal and sensitive data including name and contacts, personal views.	Microsoft 365 Lockable cabinet	Conduct business to further charitable aims	Only available to staff who need access for the purpose of their duties; differentiated permissions If data is shared, it will be anonymised	Up to 18 months
Feedback data	Name and contacts	Microsoft 365 Lockable cabinet	Conduct business to further charitable aims.	Only available to staff who need access for the purpose	Up to 18 months

			To meet contract requirements	of their duties; differentiated permissions If data is shared, it will be anonymised	

Reviewed 14.08.20 by TL and AM