DATA PROTECTION (DPA 2018) and GDPR-UK POLICY

Introduction

Personal Data and Special Category Data considered as:

Personal data is any information relating to an identified or identifiable natural person (data subject).

- Name
- Address
- Email address
- Photo
- IP address[1]
- Location data
- Online behaviour (cookies)
- Profiling and analytics data

Special Categories of personal data:

- Race
- Religion
- Political opinions
- Trade union membership
- Sexual orientation
- Health information
- Biometric data
- Genetic data

There are separate safeguards for personal data relating to criminal convictions and offences which will be outlined within this policy.

This policy sets out the obligation of Unique Voice CIC (hereafter Unique Voice) regarding data protection and all stakeholders in respect of their General Data Protection.

This policy sets out the procedures to be followed when dealing with personal data. The procedures and principles set out herein must be followed always by Unique Voice, its employees, agents, contractors, or other parties working on or behalf of Unique Voice.

Unique Voice places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses, or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). UK GDPR came into force on 1st January 2021.

UK organisations therefore have at least two data protection laws to adhere to:

- The DPA 2018 and UK GDPR if they process only domestic personal data.
- The DPA 2018 and UK GDPR, and the EU GDPR if they process domestic personal data and offer goods and services to, or monitor the behaviour of, EU residents.

Data Protection Principles

This policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

1. Processed lawfully, fairly and transparently.
2. Collected only for specific legitimate purposes.
3. Adequate, relevant and limited to what is necessary.
4. Accurate and, where necessary, kept up to date.
5. Stored only as long as is necessary.
6. Processed in a manner that ensures appropriate security.

Lawful, Fair and Transparent Data Processing

The Regulation seeks to ensure that personal data is processed lawfully, fairly and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

- If the data subject has given their consent;
- To meet contractual obligations;
- To comply with legal obligations;
- To protect the data subject's vital interests;
- For tasks in the public interest; and
- For the legitimate interests of the organisation.

The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the 'right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object
- Rights with respect to automated decision-making and profiling.

Valid consent

There are strict rules regarding consent:

- Consent must be freely given, specific, informed and unambiguous (see below regarding child age of consent).
- A request for consent must be intelligible and in clear, plain language.
- Silence, pre-ticked boxes and inactivity will no longer suffice as consent.
- Consent can be withdrawn at any time.
- Consent for online services from a child is only valid with parental authorisation.
- Organisations must be able to evidence consent.

For information purposes:
Important differences between the DPA 2018/UK GDPR and the EU GDPR

Child consent age

- EU GDPR: A child can consent to data processing at age 16.
- DPA 2018/UK GDPR: A child can consent at age 13. Please refer to DPIA (Data Privacy Impact Assessment - see Section 7 of this policy) for requirements regarding consent for individual projects.

Definition of personal data

- EU GDPR: Personal data can include IP addresses, Internet cookies and DNA
- DPA 2018/UK GDPR: More limited definition.

Processing of criminal data

- EU GDPR: Processors of criminal data must have official authority to do so.
- DPA 2018/UK GDPR: Processors of criminal data do not require official authority.

Automated decision making/processing

- EU GDPR: Data subjects have rights to refuse automated decision making or profiling.
- DPA 2018/UK GDPR: Permits automated profiling subject to legitimate grounds for doing so.

Data subject rights

- EU GDPR: Protects data subjects to personal data processing.
- DPA 2018/UK GDPR: Data subject rights can be waived if they significantly inhibit an organisation's legitimate need to process data for scientific, historical, statistical, and archiving purposes.

Privacy vs Freedom of Expression

- DPA 2018/UK GDPR: An exemption exists in relation to the processing of personal data if it is in the public interest.

Representatives

- EU GDPR: Many non-EU data controllers and processors that offer goods and services to, or monitor the behaviour of, data subjects in the EU must appoint a representative in the EU.
- DPA 2018/UK GDPR: Many non-UK data controllers and processors that offer goods and services to, or monitor the behaviour of, data subjects in the UK must appoint a representative in the UK.

Administrative fines

- EU GDPR: The maximum fine for non-compliance is €20 million or 4% of annual global turnover.
- DPA 2018/UK GDPR: The maximum fine for non-compliance is £17.5 million.

PROCEDURE

1. **PROCESSED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES**

1.1. Unique Voice collects and processes personal data set out in Section 19 of this policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates), and data received from third parties which could include consent for project participation, consent for media inclusion, contact details, curriculum vitae, regulatory licensing information specific to data subjects, purchase records.

1.2. Unique Voice only processes personal data for the specific purposes set out in Section 19 of this policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected from them, or as soon as possible (not more than one calendar month) after collection where is obtained from a third party.

2. **ADEQUATE, RELEVANT AND LIMITED DATA PROCESSING**

2.1. Unique Voice will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Section 1.

3. **ACCURACY OF DATA AND KEEPING DATA UP TO DATE**

3.1. Unique Voice shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data is checked when collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found all reasonable steps are taken without delay to amend or erase the data, as appropriate.

4. **TIMELY PROCESSING**

4.1. Unique Voice shall not keep personal data for any longer than is necessary considering the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay. Time periods for retaining data will be considered and itemised in the Record of Processing Activities (RoPA)/Document Control spreadsheet.

5. **SECURE PROCESSING**

5.1. Unique Voice shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Sections 20 and 21 of this Policy.

6. ACCOUNTABILITY

6.1. Unique Voice data protection compliance is looked after by Claire Farnham, claire@uniquevoice.org Tel: 0117 428 6240

6.2. Unique Voice shall keep written internal records of all personal data collection, holding and processing on the Record of Processing Activities (RoPA)/Document Control spreadsheet which shall incorporate the following information;

- The name and details of Unique Voice, its data protection coordinator, and any applicable third-party controllers;
- The purposes for which Unique Voice processes personal data;
- Details of the categories of personal data collected, held, and processed by Unique Voice; and the categories of data subject to which that personal data relates;
- Details (and categories) of any third parties that will receive personal data from Unique Voice;
- Details of any transfers of personal data to other countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by Unique Voice; and
- Detailed description of all technical and organisational measures taken by Unique Voice to ensure security of personal data.

7. DATA PRIVACY IMPACT ASSESSMENTS (DPIA)

7.1. Unique Voice shall carry out DPIAs when and as required under Regulation. DPIAs shall be overseen by Unique Voice's administration manager who oversees GDPR compliance and shall address the following areas of importance:

- The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
- Details of the legitimate interests being pursued by Unique Voice;
- An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- An assessment of the risks posed to individual data subjects; and
- Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

7.2. DPIAs should be sent to the administration manager and signed off. All personal data being requested is added to the RoPA.

8. THE RIGHTS OF DATA SUBJECTS

8.1. Unique Voice follows all rights of data subjects laid out by the Regulation:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the 'right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object
- Rights with respect to automated decision-making and profiling.

9. THE RIGHTS OF CHILDREN

Children have the same rights as adults over their personal data (as outlined in Section 8 above). Processing procedure is outlined in Section 19.

However, children need particular protection when collecting and processing personal data because they may be less aware of the risks involved. Such specific protection should, in particular apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. Any such data collection carried out by Unique Voice or its Agents or any online services available directly to children will be carried out/designed with regard to the Age Appropriate Design Code.

Unique Voice currently process children's data for the purposes set out in Section 19.

Consent

For the purposes of consent, in the UK, only children aged 13 or over are able to provide their own consent. In obtaining consent, as detailed in Section 19, Unique Voice will refer to the GDPR policy of the relevant school/third party referral body regarding their requirement for parental consent and will in the first instance obtain parental consent for participation by children of any age. Consent forms will request that persons with parental responsibility will discuss the use of data and ensure that the child is aware of the publication of the data. At all times, the best interest of the child will be considered.

In the case of any child over the age of 13 wishing to exercise their rights under GDPR, each case will be taken on an individual basis, age appropriate information given and clarification obtained that the child has sufficient understanding.

10. **KEEPING DATA SUBJECTS INFORMED**

10.1. Unique Voice shall ensure that the following information is provided to every data subject when personal data is collected:

- Details of Unique Voice including, but not limited to, the identity of the administration manager who oversees data protection;
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in section 19 of this Policy) and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which Unique Voice is justifying its collection and processing of personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;
- Where personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see section 22 of this policy for further details concerning such third country data transfers);
- Details of the length of time the personal data will be held by Unique Voice (or, where there is no predetermined period, details of how that length of time will be determined);
- Details of the data subject's rights under the Regulation;
- Details of the data subject's right to withdraw their consent to Unique Voice processing of their personal data at any time;
- Details of the data subject's right to complain to the Information Commissioner's Office (ICO) which is the supervisory authority under the Regulation;
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
- Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

10.2. The information set out above in section 10.1 shall be provided to the data subject at the following applicable time:

10.2.1. Where the personal data is obtained from the data subject directly, at the time of collection;

10.2.2. Where the personal data is not obtained from the data subject directly (i.e. from another party):

- If the personal data is used to communicate with the data subject, at the time of the first communication; or
- If the personal data is to be disclosed to another party, before the personal data is disclosed; or
- In any event, not more than one month after the time at which Unique Voice obtains the personal data.

11. DATA SUBJECT ACCESS

11.1. A data subject may make a subject access request ('SAR') at any time to find out more about the personal data which Unique Voice holds about them. Unique Voice is normally, required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

11.2. SARs can be made to any staff member in varying formats included via a link on the website.

11.3. All SARs received must be forward to the administration manager overseeing data protection. The process for responding to a SAR is further detailed in the SAR Procedure document.

11.4. Unique Voice does not charge a fee for the handling of normal SARs. Unique Voice reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

12. RECTIFICATION OF PERSONAL DATA

12.1. If a data subject informs Unique Voice that personal data held by Unique Voice is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt of the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for an extension).

12.2. If any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

13. ERASURE OF PERSONAL DATA

13.1. Data subjects may request that Unique Voice erases the personal data it holds about them in the following circumstances;

- It is no longer necessary for Unique Voice to hold that personal data with respect to the purpose for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to Unique Voice holding and processing their personal data;
- The data subject objects to Unique Voice holding and processing their personal data (and there is no overriding legitimate interest to allow Unique Voice to continue doing so) (see section 16 of this policy for further details concerning data subjects' rights to object);
- The personal data has been processed unlawfully;
- The personal data needs to be erased for Unique Voice to comply with legal obligation;
- The personal data is being held and processed for providing information society services to a child.

13.2. Unless Unique Voice has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

13.3. If any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

14. RESTRICTION OF PERSONAL DATA PROCESSING

14.1. Data subjects may request that Unique Voice ceases processing the personal data it holds about them. If a data subject makes such a request, Unique Voice shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

14.2. If any affected personal data has been disclosed to third parties, those shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

15. DATA PORTABILITY

15.1. Unique Voice processes personal data using automated means. Microsoft office / Apple docs files are stored on either Dropbox/ ICloud/ or an in-house server. Backups of the data are done by dropbox/ ICloud daily on the in-house server and on management level lap tops. All servers are encrypted.

15.2. Where data subjects have given their consent to Unique Voice to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between Unique Voice and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

15.3. To facilitate the right of data portability, Unique Voice shall make available all applicable personal data to data subjects in the following formats: Microsoft Word or Excel document, Pages, Numbers, PDF; JPEG

15.4. Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.

15.5. All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

16. OBJECTIONS TO PERSONAL DATA PROCESSING

16.1. Data subjects have the right to object to Unique Voice processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), [and processing scientific and/or historical research and statistics purposes].

16.2. Where a data subject objects to Unique Voice processing their personal data based on its legitimate interests, Unique Voice shall cease such processing forthwith, unless it can be demonstrated that Unique Voice's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

16.3. Where a data subject objects to Unique Voice processing their details for direct marketing purposes, Unique Voice shall cease such processing forthwith.

16.4. Where a data subject objects to Unique Voice processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to

his or her particular situation'. Unique Voice is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

17. AUTOMATED DECISION-MAKING

17.1. If Unique Voice uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from Unique Voice.

17.2. The right described in 17.1 does not apply in the following circumstances:

- The decision is necessary for the entry into, or performance of, a contract between Unique Voice and the data subject;
- The decision is authorised by law; or
- The data subject has given their explicit consent

18. PROFILING

18.1. Where Unique Voice uses personal data for profiling purposes, the following shall apply:

- Clear information explaining the profiling will be provided, including its significance and the likely consequences;
- Appropriate mathematical or statistical procedures will be used;
- Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and
- All personal data processed for profiling purposes shall be secured to prevent discriminatory effects arising out of profiling (see section 20 and 21 of this policy for more details on data security)

19. PERSONAL DATA

19.1. The following personal data may be collected, held, and processed by Unique Voice ;

- Name and other identifying information of the participant and of the person with parental control in order to confirm/refuse consent for participation in a project;
- Name and other identifying information of the participant and of the person with parental control in order to confirm/refuse media exposure/participation
- Name and private address, collected to manage recruitment, retention, rostering and invoicing;
- Qualifications and certificates, collected to determine suitability for employment;
- Information for Gov DBS checks in order for safe recruitment.
- Next of Kin name and contact details, collected to inform in the event of illness or accident
- Personal data of persons collected for contact purposes relating to contractual obligations with Unique Voice.
- Personal data of persons collected for demonstrating company social impact (anonymised).

- Personal data for reporting to funders/ commissioners (anonymised).
- Media consent for use in digital projects and/ or social media/ website content / marketing.
- Personal data for child safety within projects, such as medical, dietary, and behavioural needs.
- Personal data for child safety within projects such as registers.
- Personal data for child safety for attendance of projects such as parent/ carer contact details.

20. DATA PROTECTION MEASURES

20.1. Unique Voice shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

- All emails containing personal data must be encrypted using https;
- Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded and electronic copies should be deleted securely using 'Permanent Eraser' for Mac los and 'Easy Shred for Windows OS.
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.
- Personal data may not be transmitted over a wireless network if there is a wired alternative
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The emails itself should be deleted. All temporary files associated therewith should also be deleted;
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient;
- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of Unique Voice requires access to personal data that they do not already have access to, such access should be formally requested via the administration or office manager;
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
- No personal data may be transferred to any employees, agents, contractors or other parties, whether such parties are working on behalf of Unique Voice or not, without the authorisation of the administration or office manager.
- Personal data must be handled with care always and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time.
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period, the user must lock the computer and screen before leaving it;
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to Unique Voice or otherwise [without the formal written approval of Administration or Office manager and in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is necessary].

- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Unique Voice where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to Unique Voice that all suitable technical and organisational measures have been taken);
- All personal data stored electronically should be backed up daily. Backups are done online within Dropbox / ICloud and onto a hard drive every 3 months. All backups are encrypted.
- Unique Voice has a dedicated Digital & Social Media Policy which must be adhered to in full with regard to the transfer of images and data.

21. ORGANISATIONAL MEASURES

21.1. Unique Voice shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of Unique Voice shall be made fully aware of both their individual responsibilities and Unique Voice's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, agents, subcontractors, or other parties working on behalf of Unique Voice that need access to, and use of, personal data to carry out their assigned duties correctly shall have access to personal data held by Unique Voice;
- All employees, agents, contractors, or other parties working on behalf of Unique Voice handling personal data will be appropriately trained to do so.
- All employees, agents, contractors, or other parties working on behalf of Unique Voice handling personal data will be appropriately supervised;
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
- The performance of those employees, agents, contractors, or other parties working on behalf of Unique Voice handling personal data shall be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of Unique Voice handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;
- All agents, contractors, or other parties working on behalf of Unique Voice handling personal data must ensure that all their employees who are involved in the processing personal data are held to the same conditions as those relevant employees of Unique Voice arising out of this Policy and Regulation;
- Where any agent, contractor or other party working on behalf of Unique Voice handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Unique Voice against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

22. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK

22.1. Unique Voice may from time-to-time transfer ('transfer' includes making available remotely) personal data to countries outside of the UK.

22.2. The transfer of personal data to a country outside of the UK shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the ICO has determined ensures an adequate level of protection for personal data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the ICO; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- The transfer is made with the informed consent of the relevant data subject(s);
- The transfer is necessary for the performance of a contract between the data subject and Unique Voice (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- The transfer is made from a register that, under UK law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who can show a legitimate interest in accessing the register.

23. DATA BREACH NOTIFICATION

23.1. All personal data breaches must be reported immediately to Unique Voice's administration manager who oversees GDPR.

23.2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the ICO is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

23.3. If a personal data breach is likely to result in high risk (that is, a higher risk than that described under section 23.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

23.4. Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of Unique Voice's administration manager who oversees GDPR (or other contact point where information can be obtained);
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by Unique Voice to address the breach including, where appropriate, measure to mitigate its possible adverse effects.