Data Protection Policy for Becki Short

This policy covers any and all work carried out by Becki Short including but not limited to: singing/performing arts lessons, mentoring, peer chats, group sessions and workshops. This policy applies to anyone working for or with Becki Short, including but not limited to: students, clients, paid staff, contractors and volunteers.

Key details

Policy prepared by:	Rebecca M Short
Policy became operational on:	October 2020
Next review date:	October 2021

Introduction

I need to gather and use certain information about individuals. This can include students, clients, suppliers, business contacts, contractors and other people I work with or need to contact. This policy describes how this personal data must be collected, handled and stored to meet the data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures I:

- Comply with data protection law and follow good practice
- Protect the rights of staff, customers and partners
- Am open about how I store and processes individuals' data
- Protect myself from the risks of a data breach

Data protection law (GDPR)

The Data Protection Act 2018 describes how personal information must be collected, handled and stored. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act says that personal data must be:

1. processed fairly, lawfully and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
3. used in a way that is adequate, relevant and limited to only what is necessary ('data minimisation')
4. accurate and, where necessary, kept up to date, including ensuring that reasonable steps will be taken to erase or rectified inaccurate data without delay ('accuracy')
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 ('storage limitation')
6. handled/processed in a way that ensures appropriate security, including protection against unlawful or unauthorised processing/access, loss, or accidental destruction or damage ('integrity and confidentiality')

There is stronger legal protection for more sensitive information, such as:

- race

- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Relevant Data

This policy applies to all data that I hold relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Photo/video/audio files, where an individual is identifiable (eg. Facial or voice recognition)
- Plus any other information relating to individuals

Data Protection Risks

This policy helps to protect me from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how I use data relating to them.
- Reputational damage. For instance, I could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with me has some responsibility for ensuring data is collected, stored and handled appropriately. Anyone that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

I am primarily responsible for ensuring that legal obligations are met, including the following:

- Keeping updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies regularly.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from people covered by this policy.
- Dealing with requests from individuals to see the data held about them
- Checking and approving any contracts or agreements with third parties that may handle sensitive data.
- Ensuring everything used for data storage meets acceptable security standards.
- Performing regular checks/scans on security hardware/software for proper functionality.
- Evaluating any third-party services being considered to store or process data before using. For instance, cloud computing services.
- Approving any data protection statements attached to communications (EG: emails/letters).
- Addressing any data protection queries from journalists or media outlets like newspapers.

- Where necessary, working with other people to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy are those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, contractors can request it through the proper channels.
- Training for data handling will be provided when required
- Contractors should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Data Storage

These rules describe how and where data should be safely stored.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, paper or files should be kept in a locked drawer or filing cabinet.
- Paper/printouts should not be left where unauthorised people could see them.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location.
- Data should be backed up frequently. Those backups should be tested regularly.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use

Personal data is only of value when it is currently in use or required by law to be kept.

- Computers with personal data on must be password protected, and locked when not in use.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Personal data must be encrypted before being transferred electronically.
- Media such as photos, video and audio will be used in line with media consent agreements from individuals.

Data Accuracy
The law requires reasonable steps be taken to ensure data is kept accurate and up to date.

- Data will be held in as few places as necessary.
- Confirmation of accuracy of data will be made regularly.
- Data should be updated as inaccuracies are discovered.

Subject Access Requests/Your Rights
All individuals who are the subject of personal data held by me are entitled to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

If an individual contacts me requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to Rebecca Short at becki@beckishort.co.uk. I will aim to provide the relevant data within 14 days. I will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons
In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, I will disclose requested data. However I will ensure the request is legitimate, seeking assistance from legal advisers where necessary.

Providing information
I aim to ensure that individuals are aware that their data is being processed, and that they understand how the data is being used and how to exercise their rights.

This policy was last reviewed on: 04/10/2020 **Signed:** Becki Short