Data Protection Policy (including GDPR)

1. Introduction

Flower Skills and Training is committed to preserving the privacy of its staff and students, and to comply with the Data Protection Act (2018) and the General Data Protection Regulations.

The data protection principles are set out in the Data Protection Act (1998). Article 5 of the General Data Protection Regulation requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

- Accurate and, where necessary, kept up to date

- 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

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

2. Purpose

Flower Skills and Training processes personal data to fulfil contractual obligations, salary and benefits, holiday and sickness, funding claims, performance and achievement, safeguarding, equality diversity and inclusion, health & safety, accident reports, disciplinary, provision of education, support and advice to students and clients, to promote the services, for publications, financial and staffing records, and other statutory obligations. Processing of this data also includes the use of CCTV in order to monitor and maintain the security

of the premises and for the prevention or detection of crime. This is not an exhaustive list.

3. Personal Data

Personal data is defined as data relating to a living individual who can be identified from that data alone, or with other data held by the company or which the company is likely to receive. This includes special category data relating to an individual's gender, age, ethnicity, disability, political opinions, religious or similar beliefs, physical or mental health, sexual life, commission or alleged commission of any offence or information concerning related criminal proceedings or outcomes. The GDPR regulates the "processing" of personal information which has a very broad meaning and includes obtaining, storing, viewing, using, updating, disclosing and destroying any data held electronically, in structured manual records and to a limited extent to unstructured manual records.

The company is committed to using personal data responsibly to protect and keep secure from loss or destruction. The requirements the company has for processing personal data are recorded on the public register maintained by the Information Commissioner. The company notifies and renews the notification on an annual basis as the law requires. If there are any interim changes, these will be notified to the Information Commissioner within 28 days. Flower Skills and Training's registration with the Information Commissioner's Register of Data Controllers is: Z9154525.

4. Policy Statement

This policy outlines the responsibilities of all staff (including 3rd parties under contract, and or self-employed / volunteers) with regard to the Data Protection Act (1998) and the General Data Protection Regulation.

Staff are required to handle and process data in any of the company's records or systems in accordance with this policy and in accordance with other related policies concerning the handling or processing of data.

5. Implementation

To meet the responsibilities Flower Skills and Training will:

- Ensure any new or planned projects that involve Personal Data are preceded with a Data Privacy Impact Assessment.
- Ensure that access controls are limited to role relevance.
- Ensure any personal data is collected in a fair and lawful way.
- Gain explicit consent where required.

• Explain at the outset why information is being collected, what it will be used for and with whom it will be shared.

• Ensure that only the minimum amount of information needed is collected and used.

• Ensure the information used is up to date and accurate.

• Review the length of time information is held, in line with funder recommendations and other relevant legislation.

• Ensure information is kept safely.

• Ensure the rights people have in relation to their personal data can be exercised.

• Dispose of data appropriately and without unnecessary delay.

• Ensure that anyone managing and handling personal information is trained to do so.

• Ensure that anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do.

• Any disclosure of personal data will be in line with relevant legislation, and internal policies and procedures.

• Any sharing of data to third parties is covered by a data sharing agreement.

6. Training

The Company will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

7. Links to Other Company Policies

The following Policies and guidance are relevant to personal information.

• Information Security Policy

• Equality and Diversity Policy

• Safeguarding Policy

8. Data Security

The company has an Information Security Policy that staff must adhere to in order to ensure personal information is protected from unauthorised viewing and from loss (including computer documents, emails and paper copies by ensuring staff are provided with adequate awareness training and follow guidelines set out in the GDPR code of practice:

- Use lockable cupboards (restricted access to keys)
- Mandatory renewal of passwords to agreed frequency
- Password protection on personal information files
- Setting up computer systems to allow restricted access to certain areas
- Not allowing personal data to be taken off site (as hard copy, on laptop or on memory stick) without adequate safeguarding i.e. encryption
- If personal data can be taken off site, set out in which forms (paper, memory stick, and laptop) and give instruction to staff about keeping it safe
- Secure and reliable security back up of data
- Password protected attachments for sensitive personal information sent by email
- Robust and trustworthy IT security features
- Secure data flows across organisation and 3rd party data sharing requirements
- Robust secure IT storage facility of our electronic data
- Ensure all disposals of data are suitably destroyed.
- Ensure data is not shared without the explicit consent of the subject, where no exemptions apply.
- Set adequate access controls – role specific
- Continuous review of all measures

The company will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. All users must take reasonable responsibility to ensure the data is accurate and up to date, relevant and not excessive. Any unauthorised disclosure of personal data to a third party by any staff member may result in disciplinary or legal action. Failure to comply with company policies and procedures for handling staff/student data is a disciplinary offence which may be considered gross misconduct and may also involve personal criminal liability.

9. Data Subject Rights / Subject Access Requests

Individuals have a right under the Regulation to ask Flower Skills and Training if it holds their personal data, and if so, be provided with a copy of it. Any person wishing to exercise this right should apply in writing to the company. In order to ensure the company has met the security requirements of the GDPR, the following information will be required before access is granted: relevant identifying details including, Full name, Date of birth, National insurance number. The company may also require proof of identity. The following forms of ID will be acceptable: birth certificate, passport, or driving licence.

Subject Access Requests will be dealt with in line with the timescales set out within the GDPR. The company will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within one month as required by the Regulation from receiving the written request. The company will provide the information in a clear format that is easily understood and in a format suitable for the requesters needs. The company may request further details to clarify the exact requirements prior to the start of the one month. If an individual considers the details provided in response to a subject access request are incorrect or out of date, they should contact the company immediately.

Anyone whose personal information the company processes has the right to know:

- What information the company holds and processes about them
- The legitimate reasons for processing
- The right to consent or withdraw consent
- How to gain access to this information
- How to keep it up to date
- To receive this data in a clear format
- To receive this data within one month
- Data Subjects have the right to prevent processing of their personal data in some circumstances and have the right to correct, rectify, block or erase information regarded as incorrect
- To be informed of any miss use or loss of this data if the loss represents a high risk to the rights and freedoms of individuals
- The right to erasure of personal information – commonly referred to as the right to be forgotten

• The right to complain and/or seek compensation It is a criminal offence under the GDPR for any user to alter, illegally access, deface or remove any record (including e-mails) following receipt of an information request. The company will take necessary action against any individual who is found to have carried out this act, which may result in disciplinary or legal action. Other Criminal acts under GDPR may also result in disciplinary or criminal proceedings; definitions can be found at www.ico.org.uk

If you have any queries or concerns regarding Flower Skills and Training's management of personal data then you can contact the company directly. Any comments or complaints will be dealt with through the company complaints procedure. The company will maintain records of all complaints and their outcome. If you are still unhappy after having made a complaint individuals can contact the Information Commissioner through their website: www.ico.org.uk .

10. Data Sharing

There are occasions when it is necessary for the company to share data with other organisations or people and where consent is required the company will seek and gain this from the Data Subject except where lawful bases for processing data exist, including:

• In order to fulfil legal obligations, including but not limited to:

- where it is necessary for carrying out rights and obligations under employment law;
- Pay and benefit details HM Revenue and Customs
- UK Border Control
- Police or other law enforcement or investigatory institutions;

• Where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;

• Where you have made the data public;

• Where processing the data is in the legitimate interests of the company, including but not limited to sharing the data with:

- Other Educational bodies or institutions
- Careers Services / Connexions
- Education and Skills Funding Agency
- Internal and external audit
- Where processing is necessary for the establishment, exercise or defence of legal claims;
- Where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity, and

- Research purposes where data has been fully anonymised. For further information, access the website of the Information Commissioner's Office: https://ico.org.uk/

11. Retention and Disposal of Data

The company will retain information about staff and students for as long as is reasonable and necessary to comply with the law and for legitimate business needs. This will include information needed in connection with administering pensions and taxation, for potential or current disputes or litigation regarding employment, in the case of job applicants, in relation to any complaints or claims regarding the selection process, and information required for job references. For students this will include information needed in connection with administering student applications, enrolment, attendance, achievement, success, post-training destinations, personal tutor notes, academic records, and information required for references, and in the case of prospective students, in relation to any enquiries, applications and interviews.

The company will dispose of data in line with the company's Data Retention Policy written in conjunction with sector-recommended data retention principles and any legal and funding audit requirements. Once the retention period has elapsed, the company will ensure that any information is destroyed by secure means, i.e. by shredding, pulping or burning for hard copy, deletion etc. for electronic/digitised copy.

12. Data Security Breach Procedure

The company takes the risk to security loss very seriously and adheres to the legal framework set down by the Information Commissioner's Office and industry standards. The company has a Breach Management Procedure to be followed in the event of a data breach or suspected data breach to ensure the company responds and manages effectively any breach in line with the GDPR recommendations. Actions may include:

• Containment and recovery – the company will respond to the incident immediately which includes a recovery plan and, where necessary, implement procedures for damage limitation.

• Assessing the risks – the company will assess any risks associated with a breach, as these could affect any procedures after the breach has been contained. In particular, the company will assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to re occur.

• Notification of breaches – if appropriate the company will inform a Data Subject about an information security breach, the ICO; other regulatory bodies; other third parties such as the police and the banks.

• Evaluation and response – the company will investigate the cause of the breach and also evaluate the effectiveness of any response made. If necessary, the company will update its policies and procedures accordingly

13. International data transfers

We will not transfer personal data to countries outside the EEA.

Last reviewed: May 2018
Next review: May 2020