The Talent Foundry

Data Protection Policy

December 2019

Date of last review by the Board: 20th June 2018

Next review date: Summer Term 2020

KEY FACTS:

Policy Objective

This policy provides guidance in respect of data protection and the use of personal data at The Talent Foundry Trust.

Scope

This policy applies to all The Talent Foundry Trust employees, workers, contractors and interns who have access to personal data and are made aware of this policy.

1 INTRODUCTION

1.1 This Data Protection Policy sets out the roles, responsibilities and procedures around the use of personal data at The Talent Foundry Trust (TF)

1.2 This policy applies whenever you are collecting or handling personal data (as defined in paragraph 3.2) in any way.

1.3 Everyone has rights with regard to the way in which their personal data is handled. In the course of our activities we will collect, store and use personal data about staff, workers, contractors, interns, students, teachers and other people in external organisations.

1.4 This policy applies to all TF employees. Any breach of this policy may result in disciplinary action / termination of services by TF as appropriate.

1.5 This policy does not form part of any employee's contract of employment and may be amended at any time.

1.6 Please read this policy alongside our Data Retention Policy.

2 AIMS OF THIS POLICY

2.1 To protect the rights, safety and welfare of individuals, including children, in relation to the use of personal data within TF.

2.2 To help you understand the fundamentals of data protection law.

2.3 To guide you to help ensure that TF is compliant with data protection laws.

2.4 To understand the risks to TF of non-compliance with data protection laws.

3 WHAT DOES THE LAW SAY?

What is the GDPR?

3.1 The General Data Protection Regulation 2016/679 (**"GDPR"**) is applicable to all EU Member States as of the 25 May 2018. In the UK, the GDPR replaces the Data Protection Act 1998 (**"DPA"**). We anticipate that, prior to the United Kingdom leaving the European Union, a new Act will be enacted by parliament which will implement fully the GDPR into UK legislation (we will refer to this collection

of laws together with any other applicable data protection laws and regulations as the **"Data Protection Laws"**). The GDPR will have a major impact on how we store and use personal data. The aim of the new law is to give individuals new rights over their data. These include things such as the right to be erasure. We have added a more detailed explanation of these rights below.

What is personal data?

3.2 Personal data is any data which relates to a living individual who can be identified from that data (or from that data and other information likely to come into TF's possession). It therefore captures a wide range of data. Examples of personal data are set out in the Schedule at the end of this policy. If you are unsure about whether certain information is personal data or not, please speak with the Operations Director or CEO.

What is sensitive personal data?

3.3 The Data Protection Laws class a certain type of personal data as sensitive personal data. A list of examples of sensitive personal data are also set out in the Schedule. It is important that you recognise what sensitive personal data is because the law imposes more stringent requirements around use of sensitive personal data and possibly means you need to get the consent from the individual whose sensitive personal data you are using before you are lawfully permitted to use it.

Who regulates the GDPR in the UK?

3.4 In the UK, the Data Protection Laws are independently enforced by the Information Commissioner's Office (**"ICO"**).

What happens if we get it wrong?

3.5 The ICO has a wide range of powers. It can issue enforcement notices where it tells businesses to remedy a certain breach. It can also publicise data protection breaches on its website which could lead to negative publicity for TF if we are in breach. It also has the right to audit TF and fine TF up to €10 million or 2% of global turnover for breaches of the Data Protection Laws.

The 6 data protection principles

3.6 The GDPR sets out 6 data protection principles which you should be aiming to follow at all times; they are as follows:

(1) **Fair, lawful and transparent.** The first principle is that personal data shall be processed fairly, lawfully and transparently. The Data Protection Laws are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individuals whose data you are using. It also important to be transparent with individuals in relation to what you do with their data.

(2) **Use it only for a limited purpose.** The second principle is that personal data shall be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes. As a member of staff at TF you may be involved in collecting personal data in different ways. This may include data you receive directly from individuals (for example, by completing booking forms for specific programmes) and data you receive from other sources (including, for example, information from teachers or references from past employers for employees). You must not use the data for your own personal purposes. Personal data which you collect in the course of your

employment, or provision of services, should be used strictly as part of carrying out your role at/ for TF and only for the purpose for which it was collected.

(3) **Data minimisation.** The third principle is that personal data shall be adequate, relevant and limited to what is necessary. You should only collect, use, access or analyse personal data to the extent that you need to.

(4) **Accuracy.** The fourth principle is that personal data shall be accurate and, where necessary, up to date. You should check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You should take all reasonable steps to destroy or amend inaccurate or out-of-date data.

(5) **Data retention.** The fifth principle is that personal data shall be kept for no longer than is necessary. The Data Protection Laws do not tell us how long is necessary. TF has a separate Data Protection Retention Policy to guide you in determining how long to keep certain types of information. Please refer to that policy for further details about how long you should be keeping certain types of personal data and how you should be deleting personal data. It is important that you follow the Personal Data Retention Policy and it should be read in conjunction with this policy.

(6) **The security (or "ATOM") principle**. The sixth principle is that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful use of personal data and against accidental loss, destruction or damage. The GDPR says that we must use "appropriate, technical and organisational measures" (ATOM) to keep data secure. Security of personal data applies to a range of areas, including IT security, and it should be applied throughout your day-to-day activities. You should review TF's IT policies for further details about using IT securely.

3.7 There are additional principles that we believe are just as important as those set out above and these are set out below.

Respecting the individual's legal rights. TF will also be required to process personal data in accordance with the rights of data subjects (i.e. the individuals about whom TF holds personal data). Please see paragraphs 9 and 10 for further detail about individuals' right of access to the information TF holds about them (commonly known as a subject access request or **"SAR"**) and their right for information about them to be erased (typically referred to as the right to erasure or right to be forgotten).

Don't let personal data leave the UK without telling us. Personal data must not leave the European Economic Area unless certain legal protections are in place. If you would like further details about this principle or have any queries, please speak to the Operations Director (see paragraph 4). If you are aware of personal data being transmitted outside of the UK, you need to tell the Operations Director. This might mean having to do some investigation as to how personal data flows in and out of the organisation.

Accountability. Everyone needs to take responsibility for the principles above and be able to demonstrate that we are complying with them. Please make sure that you are in a position to show the Operations Director or CEO how you are complying with this policy and the Personal Data Retention Policy.

4 WHO CAN I SPEAK TO ABOUT DATA PROTECTION ISSUES AT TF?

TF's Data Protection Officer

4.1 TF has appointed a Data Protection Officer (**"DPO"**) who is responsible for overseeing compliance with the Data Protection Legislation and with this policy. That post is held by the Operations Director, Susannah French Susannah.french@talentfoundry.org.uk Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Operations Director.

5 TAKING OWNERSHIP

5.1 The GDPR introduces a new concept called data protection by "**design and default"**. It essentially means that we all have a responsibility to proactively build the principles (set out in paragraphs 3.6 and 3.7 above) into our everyday activities. Please ensure that you question current or old practices or technology if you think they do not follow good data protection practice and raise any issues or concerns with the Operations Director or CEO.

6 NEW IDEAS?

6.1 You may want to introduce something new and innovative to the organisation. It could be a new piece of technology or you may be looking to introduce a campaign which involves the use, in some way, of personal data. Or you might want to implement a new piece of software.

6.2 It is important that, before implementing anything new involving or impacting upon personal data, you speak with the Operations Director. Under the new GDPR concept of data protection by design and default (please see paragraph 5), we need to ensure that we have built good data protection practice into any new idea before implementing the idea. Sometimes, this will require a formal data privacy impact assessment (with which the Operations Director will provide assistance) where the new idea is potentially high risk to the privacy of our stakeholders and/or members of staff.

7 DATA BREACHES

7.1 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. It also means that a breach is more than just about losing personal data. (More information can be found at hTFps://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) The breach could be as a result of a cybercrime. Or It could be that you, or someone you know, have accidentally shared personal data with another organisation or person without permission.

7.2 If you become aware of a personal data security breach you must inform the Operations Director **immediately** by e-mail, providing as much background detail as possible.

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

7.3 If you do need to report it, the GDPR requires TF to report personal data breaches to the regulator within 72 hours of first becoming aware of it. **Please do not report the breach to the ICO yourself.**

Please contact the Operations Director or CEO for further assistance. They will assist you with completing the breach notification form which will be sent to the ICO.

8 SHARING INFORMATION WITH OTHER ORGANISATIONS

8.1 If you are looking at engaging with any new supplier, and you know that the supplier will be obtaining personal data relating to TF members of staff or other groups of people, you will need to contact you're the Operations Director or CEO as soon as possible before engaging with that supplier.

8.2 The GDPR requires TF to (a) vet these suppliers to ensure that they offer an appropriate level of security of personal data and (b) make sure that there is a written contract between the supplier and TF and that it is GDPR-compliant before being signed.

9 DEALING WITH SUBJECT ACCESS REQUESTS

9.1 A subject access request (**"SAR"**) is a written request from an individual to obtain information TF holds about him or her. This is a statutory right, however, it is not without its complications and it doesn't just mean disclosing every piece of information, because there might be legal reasons to withhold certain information. The individual issuing a SAR could be a pupil, parent and/or guardian of the pupil, member of staff or member of the public. Not everyone who requests personal data will be entitled to receive it, therefore, it is important we verify an individual's right to receive personal data, particularly where the personal data is not about themselves.

9.2 As there are strict time periods for complying with a SAR (1 calendar month from the date of the SAR), it is important that you **immediately** notify the Operations Director or CEO who will then assist with the request accordingly. **Please do not respond to the individual without first consulting with the Operations Director or CEO**.

10 RIGHT TO ERASURE REQUESTS

10.1 A right to erasure request is a written request from an individual to erase information TF holds about him or her. Like SARs, this is a statutory right but not as straightforward as you might think and it doesn't just mean deleting every piece of information about the individual because there might be legal reasons to keep certain information. As with SARs, please make sure that you contact the Operations Director or CEO **immediately** before responding to the individual making the request. **Please do not respond to the individual without first consulting with the Operations Director or CEO**

11 CHANGES TO THIS POLICY

11.1 We reserve the right to change this policy at any time. Where the changes are significant, we will make sure that we tell you about them.

SCHEDULE

EXAMPLES OF PERSONAL DATA

Personal Data	**Sensitive Personal Data**
Name (first name or last name)	Religious expression
Age	Physical or mental condition
Address	Political views and beliefs
Phone number	Racial or ethnic origin
Email address	Criminal record checks
Photograph	Trade union membership
Location	Sex life
Opinion	Sexual orientation
Bank details	Biometric data (e.g. information obtained from fingerprint or retina scanning)
Salary	Child protection files will most likely contain sensitive personal data.
Student records	Information relating to special education needs will be sensitive personal data
Letters*	
Contracts*	

*May contain personal data.

Please note that this is not an exhaustive list.