Data Protection Policy

Rev 2 25/03/2015

Document Status

This document replaces the data collection and retention policy, to be used as guidance and to state the responsibilities of Develop and its employees. This document may be copied and reproduced but the master document will be the version that resides on the company intranet, the revision being that shown on the document control register.

Contents.

1. Introduction

1.1 Background

1.1.1 Develop needs to collect personal information about people with whom it deals in order to carry out its business and provide its services.
Such people include learners, staff within other organisations, employees (present, past and prospective), volunteers, and other business contacts. The information includes name, address, email address, data of birth, contact telephone numbers, private and confidential information and sensitive information.
In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law.(for example H&S law)
No matter how it is collected, recorded and used (for example on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 1998 (DP Act).

1.1.2 The lawful and proper treatment of personal information by Develop is extremely important to the success of our business. In order to maintain the confidence of our stakeholders we ensure that Develop and its employees treat personal information lawfully and correctly.

1.2 **Data Protection Principles**

1.2.1 Develop fully supports and complies with the eight principles of the DP Act which are summarised below:
1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained/processed for specific lawful purposes.
3. Personal data held must be adequate, relevant and not excessive.
4. Personal data must be accurate and kept up to date.
5. Personal data shall not be kept for longer than necessary.
6. Personal data shall be processed in accordance with rights of data subjects.
7. Personal data must be kept secure.
8. Personal data shall not be transferred outside the European Economic Area (EEA) unless there is adequate protection. For Develop this is further refined to Outside of the UK.

2. **Scope**

2.1 The following Develop offices and those of First Place Training where Develop provides governance are within the scope of this document:

- Develop Ampthill;
- Develop Norwich;
- First Place Training Bedford;
- First Place Training Kempston;
- First Place Training Dunstable;
- Temporary Outreach settings

along with the staff working in or on behalf of Develop (this includes contractors, temporary staff, volunteers, secondees and all permanent employees).

3. **Roles and Responsibilities**

3.1 Develop will:-

- ensure that there is always one person with overall responsibility for data protection. This person is the CEO who delegates the function and implementation to the Data Protection Officer.
- provide training for all staff members who handle personal information
- provide clear lines of reporting and supervision for compliance with data protection
- carry out regular checks to monitor and assess processing of personal data and to ensure that the notification to the Information Commissioner is updated to take account of any changes in processing of personal data, trade names or registration details.
- create and maintain DP Act procedures to cover roles and responsibilities, data collection, data retention, notification, subject access requests, data sharing protocols, requests by the Police or HRMC, training and compliance testing
- ensure that employees are aware of their responsibility for the DP Act by adding it their roles and responsibilities.
- treat requests for the release of data under part IV of the DP Act, (exemptions) on a case by case basis.

3.2 **Employee Responsibilities**

3.2.1 All employees will, through appropriate supervision, instruction and training and responsible self management:

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.
- Understand the purposes for which Develop or First Place Training uses personal information.
- Collect and process appropriate information in accordance with the purposes for which it is intended.
- Ensure the accuracy of information input into systems.
- Ensure that information is securely destroyed, in accordance with the provisions of the DP Act or data retention protocols, when it is no longer required.
- On receipt of a request from an individual for information held about them, a Subject Action request (SAR), will immediately notify the Data Protection Officer.
- Not send any personal information outside of the United Kingdom without the authority of the Data Protection Officer.
- Understand that breaches of this Policy may result in disciplinary action, including dismissal.

4. **Distribution and Implementation**

4.1 **Distribution Plan**

4.1.1 This document will be made available to all Staff via the Intranet site as a reading exercise. (Initial distribution and issue of revisions should follow a standard distribution procedure that includes evidence of employee awareness)
4.1.2 Global notices will inform of subsequent revision releases and where required training in that new release will be provided as a workshop or reading exercise, in both cases training will be recorded against employee training files.

4.2 Training Plan

4.2.1 A training needs analysis will be undertaken with Staff affected by this document.

4.2.2 Based on the findings of that analysis appropriate training will be provided to staff on a tiered approach, Directors, Managers, Project Managers, administrators/data input operatives, all other staff.

4.2.3 Guidance about Data Protection will be provided on the Intranet.

5. **Monitoring**

5.1 Compliance with the policies and procedures laid down in this document will be monitored pro-actively through a schedule of audits and reactively after identified weaknesses, supported by independent reviews by both Internal and External directors on a periodic basis.

5.2 The Data Protection Officer is responsible for the monitoring, revision and updating of this document.

6. Information Communication Technology (ICT) security

6.1 A large proportion of personal data processed, viewed and held is completed with the use of ICT equipment, including but not limited to, Fax, PC's, server networks, the internet, e-mail, cloud spaces, mobile devices and remote storage devices. The security strategy for all IT equipment is taken from the IT Policy.

7. Associated Documents

7.1 The following documents relate to this policy:

Freedom of Information, Privacy and Electronic Communications Regs, DPA
Auditing and Inspections
IT Policy
Acceptable Use of ICT Policy
Data Protection Procedures
Exemptions Under Part IV Section 29

Policy signed by CEO: Mark Pike Date: 09/11/2016