DATA PROTECTION POLICY

Date Completed:	**January 2020**
Date Approved:	**January 2020**
Approved by:	**Board of Directors**
Implementation Date:	**February 2020**
Date for Review:	**January 2021**

Data Protection Policy

1. Introduction

Elite Pathways is committed to a policy of protecting the rights and privacy of individuals (which includes students, staff and others) in accordance with the Data Protection Act. Elite Pathways needs to process certain information about its staff, students and other individuals it has dealings with for administrative purposes. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff and students of Elite Pathways. Any breach of the Data Protection Act 1998 or this Data Protection Policy is considered to be an offence and in that event, the Elite Pathways disciplinary procedures may apply.

2. Scope

This policy applies to all learners and employees of Elite Pathways.

Breaches of this policy will be managed through the Elite Pathways Disciplinary policy and procedure.

This policy underpins Elite Pathway's core values and will be used objectively and free from discrimination in accordance with the Elite Pathways Equality and Diversity policy.

3. Background to the Data Protection Act 1998

The Data Protection Act 1998 enhances and widens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

4. Definitions (Data Protection Act 1998)

Personal Data - Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, and id number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive Data - Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller - Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject - Any living individual who is the subject of personal data held by an organisation.

Processing - Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data Accessing, altering, adding to, merging, deleting data Retrieval, consultation or use of data Disclosure or otherwise making available of data.

Relevant Filing System - Any paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

5. Responsibilities under the Data Protection Act

Elite Pathways as an organisation is the data controller under the new Act.
The Data Administrator acts as the Data Protection Officer and is responsible for day-to-day data protection matters and for developing data protection awareness.

All staff in managerial roles are responsible for developing and encouraging good information handling practice within the organisation.

Compliance with data protection legislation is the responsibility of all members of Elite Pathways, who process personal information.

Members of Elite Pathways are responsible for ensuring that any personal data supplied to Elite Pathways are accurate and up-to-date.

Data Protection Principles

1. All processing of personal data must be done in accordance with the eight data protection principles.
2. Personal data shall be processed fairly and lawfully.
3. Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.
4. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.
5. Data obtained for specified purposes must not be used for a purpose that differs from those.
6. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.
7. Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.
8. Personal data shall be accurate and, where necessary, kept up to date.
9. Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate.
10. It is the responsibility of individuals to ensure that data held by Elite Pathways are accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken, as an indication that the data contained therein is accurate.
11. Personal data shall be kept only for as long as necessary.
12. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.
13. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of

data.

14. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

13. Data Subject Rights

Data Subjects have the following rights regarding data processing, and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision taking process that will significantly affect them.
- To prevent processing likely to cause damage or distress.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.

14. Consent

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. Elite Pathways understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them.

Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained where this data disclosure arises outside of routine data capture such as registration.

If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

15. Data Security

All staff are responsible for ensuring that any personal data (on others), which they hold, are kept securely and that they are not disclosed to any unauthorised third party. All personal data should be accessible only to those who need to use it. Staff should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access, or
- In a locked drawer or filing cabinet, or
- If computerised, password protected, or
- Kept on disks which are themselves kept securely.
- Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left

unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff and students who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data at home or in other locations.

16. Data Disclosure

Elite Pathways must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and students should exercise caution when asked to disclose personal data held on another individual to a third party.

17. Retention and Disposal of Data

Elite Pathways discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and students. However, once a member of staff or student has left the institution, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.