1. Purpose

1.1 The purpose of this policy is to set out the principles to be followed to ensure a consistent and effective approach to managing a breach in the security of data across More Training.

2. Scope

2.1 This policy applies to all staff, learners, contractors and third-party agents handling More Training Information and information systems.

2.2 This policy applies to all data which may include personal information about people and non-personal information which could be sensitive or commercial e.g. financial data.

3. Policy Statement

3.1 More Training has an obligation to comply with relevant statutory, legal and contractual requirements. This Data Security Breach Policy is part of the Information Security suite of policies, designed to ensure data security incidents are reported promptly and managed properly to mitigate any risks to the confidentiality, integrity and availability of More Training Information and information systems.

3.2 Care should be taken to protect all data and data systems from incidents (either accidental or deliberate) that could compromise their security.

3.3 All individuals who access, use or manage More Training's Information and information systems are responsible for reporting incidents of data security breach. See PI 020 Data Security Breach incidents Procedure.

3.4 Failure to adhere to this policy will be addressed by necessary disciplinary actions in accordance with More Training's Staff Disciplinary Procedures, Student Disciplinary Procedures and relevant contractor and third-party contractual clauses.

4. Definition of an incident

4.1 An incident in the context of this policy is an event which has caused or has the potential to cause unauthorised disclosure of and/or damage to More Training

Information, information systems or reputation. Examples of an Information Security Breach are:

4.1.1 Accidental loss or theft of sensitive or personal data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick).

4.1.2 Unauthorised or accidental use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems).

4.1.3 Unauthorised or accidental disclosure of sensitive or personal information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal data posted onto the website without consent.

4.1.4 Damage or destruction or loss of personal data, or accidental or unlawful alteration of personal data (e.g. due to failure of equipment, or changes or deletions made by staff of documents on shared drives or More Training systems).

4.1.5 Compromised user account (e.g. accidental disclosure of user login details through phishing).

4.1.6 Failed or successful attempts to gain unauthorised access to More Training Information or information systems.

4.1.7 Equipment failure resulting in the non-availability of data.

4.1.8 Malware infection.

4.1.9 Disruption to or denial of IT services

Unless there are any changes this policy will be reviewed annually at the end of the academic year (1st Aug – 31st Jul) by the Owner.