Storage and transportation of learner records and assessment materials policy

1.0 Introduction

1.1 Training centres depend on information to manage services
and to provide and improve processes. Information has to be protected from misuse, loss or damage. It is necessary to ensure that confidential information that can be linked to an individual (learner, staff or visitor) is transferred, stored or disposed of securely. Cobra UK has obligations under law, local and national policy.

2.0 Purpose

2.1 The purpose of this policy is to give clear guidance to those who are processing confidential information as part of their day to day duties so that they may comply with the various related legislation, regulation and standards that apply and confidently and securely process confidential information within and out with Cobra UK boundaries.

2.2 This document sets out the practices and procedures staff must follow when transferring, storing and disposing of confidential information within and out with Cobra UK.

2.3 The principles and guidance contained within this document are not intended to be restrictive in nature but instead should enhance and encourage best practice, thus protecting the confidential information that has been entrusted to Cobra UK learners, staff and their representatives.

3.0 Scope

3.1. The policy covers the transferring, storage and disposal of confidential information held on any paper or electronic format (e.g. handwritten notes, learner/staff files, health records, letters, memos, fax, email, short message service (SMS) and texting, audio or video tapes, desk top and laptop computers and storage media such as USB memory sticks, floppy disks, CD's and backup tapes). The policy is applicable to all staff that process confidential information.

3.2 This policy relates to the verbal, physical and electronic transfer of data within and out with Cobra UK.

4.0 Definition of Terms

4.1 Confidential Information – Personal identifiable information and business sensitive information relating to learners, staff, visitors and their representatives.

4.2 Personal identifiable information – Any type of information that identifies a person and which tells you something personal about that individual. Some common identifiers are name, address, date of birth, postcode, and gender.

4.3 Business sensitive information – Any trade secret or information of a commercial nature which if released to the wrong people could damage or prejudice the commercial interests of Cobra UK or their suppliers or contractors.

4.4 Mobile Devices – e.g. Laptops, Smartphones / iPhones, iPads, tablets.

4.5 Removable Media – e.g. CD's, DVD's, Tapes, Floppy Disks, USB Sticks

4.6 Information Asset Owner – A member of staff in each

department/team/function who is responsible for registration, compliance, access and maintenance of information assets that hold confidential information.

5.0 Roles & Responsibilities

5.1 Overall responsibility for the security of information is vested with the Centre Manager, Sarah Carvell.

5.2 Senior Information Risk Owner (SIRO), by delegation from the Chief Executive takes overall ownership for organisational information risk. For the purposes of this policy, SIRO is the Centre Manager.

5.3 The responsibility for protecting the confidentiality of learner identifiable information rests with the Centre Manager.

5.4 It is the responsibility of all individuals working within Cobra UK to ensure the transferring, storing and disposing of confidential information is being carried out in line with the guidelines and procedures within this policy document.

5.5 All staff members are expected to take personal and professional responsibility for dealing securely with any confidential information they have access to in the course of their duties.

5.6 The Centre Manager is responsible for ensuring that there is regular review of this policy.

5.7 Failure to comply with the guidelines and procedures within this document

may result in disciplinary procedures being applied.

6.0 General Principles

6.1 Keep confidential information held on any format secure at all times.

6.2 Never leave confidential information held on any format unattended in any public areas.

6.3 Always practice a clear desk routine. All confidential information held on any format should be locked away when not in use.

6.4 Keep rooms, cupboards; drawers containing confidential information locked when not in use. Keys should be kept in a secure location.

6.5 Always consider anonymisation of personal identifiable information where possible. Information is said to be anonymised when identifiers; such as name, address, full postcode and any other detail that might identify an individual are removed.

6.6 If anonymisation is not appropriate consider coding the personal identifiable information, keep the code separately in a secure location.

6.7 Always use the minimum volume of identifiable information for your requirements.

6.8 Review your processes regularly to justify the need to store or transfer confidential information in any format.

6.9 When confidential information is no longer required for business purposes it must be destroyed securely following the approved destruction procedures,

see Section 11.

7.0 Verbal Communication of Confidential Information

7.1 Care should be taken when discussing confidential information to ensure that

conversations are not overhead by others who have no direct involvement with the discussions taking place. Disclosure of confidential information in this way would constitute a breach of confidentiality. This would also apply outside working hours as the duty of confidence under law would still be applicable.

7.2 When communicating confidential information via telephone staff should satisfy themselves that the information is being shared securely. Best practice involves verifying the identity of the caller and then calling the recipient back on a verified number. Care should also be taken as to who may overhear telephone conversations.

7.3 Where possible, when discussing personal identifiable information, the names of learners / staff members should be omitted from the conversation, identity should be confirmed using the course date or similar.

8.0 Physical Records Transfers and Storage

8.1 Packaging

8.1.1 A number of handling and transportation packaging methods are employed for the secure transfer of physical records within Cobra UK areas and to partner organisations. These include:

a) Single record envopak carriers with seals,

b) Multiple record envopak carriers with seals,

d) Double brown paper envelopes,

e) Brown paper and string,

f) Purpose designed plastic boxes with seals,

g) Non-tearable textured envelopes,

h) Lockable containers.

8.1.2 Transportation packaging methods employed must be fit for the purpose, they should be sufficient to protect the contents from damage and where applicable conform to manufacturer's specifications.

8.1.3 Ensure that a privacy marking is clearly visible on the package, using the following markings;

'Confidential – Learner Information' for Learner Records

'Confidential – Staff Information' for Staff Records

'Confidential - Business Information' for Business sensitive information

Ensure that the package is clearly addressed to the recipient that it is intended for.

8.1.4 When using window envelopes it is imperative to respect the privacy of the individual concerned and all staff must be aware of the necessity to ensure that no information, apart from the name, address and privacy marking, is visible through the window of the envelope.

8.2 Delivery Methods

8.2.1 Hand delivery should be utilised whenever possible.

8.2.2 All confidential records transferred out using any of the transportation methods described above must be sent by 'Recorded Delivery', 'Special Delivery' or an approved 'Special Courier' where information is recordable and traceable.

8.2.3 On no occasion should internal transit envelopes be used for the transportation of confidential information.

8.2.4 Transported items that contain confidential information must never be deposited and left unattended in areas that are not secure i.e. entrances, corridors, stairways. This includes confidential waste bags.

8.2.5 When delivery is carried out by 'Special courier staff must ensure that they are using an 'approved' special courier company with which the organisation holds a contract for service. An electronic alternative to the physical transportation may present a more secure method; see Section 9.

8.2.6 Only transport confidential information in vehicles if there is no other alternative method; for instance secure email, access by a networked shared drive etc. see Section 9.

8.2.7 Never leave paper records and/or mobile devices/media containing confidential information unattended in vehicles for extended periods. If you need to leave information of this nature in an unattended vehicle for a short period of time then ensure that it is locked away in the vehicle out of sight.

Always use the boot of your vehicle if it has one.

8.2.8 Paper records should only be taken out with your work location at the agreement of your line manager and where this is absolutely necessary tocarry out your legitimate duties.

8.2.9 Tracker systems should be adequately applied to ensure that there is always record of the whereabouts and who is responsible for that paper record at that time.

8.2.10 Records must be stored and carried in a secure bag/case. Records must not be carried 'loosely' as this increases the risk of dropping them and losing something.

8.2.11 Paper records should only be taken out with your work location for the minimum period of time, all paper records should be returned to your base as soon as possible. It is anticipated that the absolute maximum period of time paper records would be taken out with your work location is for a period over one weekend and this is only where it is absolutely necessary to facilitate delivery of your legitimate duties for instance first thing on a Monday morning.

Staff must have the agreement of their line manager if it is necessary for them to work in this way.

8.2.12 There may be exceptional circumstances that means that this is not possible i.e. if a member of staff goes off sick before returning the paper records. In this situation the records should be returned as soon as is practically possible.

Managers may have to make arrangements to retrieve records if they are required whilst the member of staff is off for a period of time.

8.2.13 Paper records must not be held out with your work location for extended periods of time, this is a breach Cobra UK policy.

8.2.14 Paper records should not be stored in your vehicle overnight, whenever possible return all items to your work location and store them securely. If this is not practicable then you must remove the items from your vehicle and store them securely within your place of residence.

8.2.15 You are responsible for any paper records that you have taken out with your work location, you must ensure that security and confidentiality of all information in your possession at all times.

8.2.16 Where health board vehicles are used for the transportation of confidential information items and the vehicle is parked on NHS premises overnight, at the end of each day the vehicle must be emptied of all such items to a secure storage location.

9 Reporting & Registration

9.1 Any suspected or actual information security breach involving confidential information must be reported to the centre manager in line with the Reporting and Managing an Information Security Breach Procedure. Staff must also report these incidents to their line manager as soon as they are discovered.