Data Security Policy and Procedures

This document sets out the policy and procedures for the protection of Data at Park Education and Training Centre including GDPR regulations.

Access to Park Education and Training Centre Network Systems

Access to at Park Education and Training Centre Central Management Information, email and Data Servers are password protected at all times and only registered users are permitted access to the system. Computers used for training or those for learner/public access will not have access to organizational, staff, learner or MI records. Login and password details must not be passed on to any other person. When a user leaves Park Education and Training Centre employment/service their login to all systems will be suspended and then deleted after one month.

Passwords must be robust see Appendix 1. If a password is forgotten it can be reset by the System Administrator. Passwords must not be written down and must not be communicated by e-mail.

User IDs do not grant administrator rights, and users without administrator rights will not have access to system files nor will they be able to install software on any computer.

Any known breach of these access rules should be reported immediately to the Centre Manager.

Data Breach Reporting

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are a result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

When a personal data breach has occurred, including at a subcontractor, it should be reported immediately to the Centre Manager who will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If there is a risk then the breach must be reported to ICO within 72 hours either by telephone or using the online form.

If it is assessed that it is not a risk to people's rights and freedoms and not reportable, the rationale will be reported in the GDPR folder.

Data and System Back Up

Data back up is carried out regularly to provide redundant failure capability. All backups are to be conducted by the Centre Manager and stored in a secure, remote location.

Laptops

All laptop computers are password protected and general users do not have access to system set-up files or programs. Laptops are set up with a separate administrator user ID and password which will not be given to any staff member, learner or other person without the express permission of the Centre Manager.

Confidential company or learner information must only be loaded onto laptop computers which are encrypted.

All laptops are to be marked as the property of Park Education and Training Centre. Central asset registers are kept of all ICT equipment, including laptops.

Transfer or Transportation of Data

Any electronic transfer of data must be by secure connection, and any data transferred must be password protected and/or encrypted and only transferred to previously approved recipients by authorised staff members.

Transportation of confidential company or personal data on any portable device (e.g. laptops, portable hard drives, memory sticks, etc.) is expressly forbidden without the prior permission of the Centre Manager. If such transportation is authorised, the data must be encrypted and/or password protected, and the device must not be left unattended at any time. In the event that any theft or unauthorised access to the data is suspected, it must be reported immediately to the Centre Manager for remedial/recovery action.

Paper Records and Digital Media Files

The transfer of personal and sensitive data in hard copy is not permitted unless prior agreement is received from the relevant authority. Should documents be sent by post, they should be double-enveloped with the internal envelope marked 'PROTECT – PRIVATE' . The envelope should be posted by special delivery or trusted courier.

Access to any learner/client information stored as paper records, including application forms, learning plans, portfolios, etc. may only be made by authorised staff and previously authorised external parties such as auditors, inspectors and awarding body staff, as appropriate. All learner/client paper records must be kept in locked fire-resistant cabinets when not in use and not left unattended when in use.

Administration office must be locked when reception staff are not present and outside of normal office hours. Except for previously authorised purposes, learner/client paper records are not to be taken out of Park Education and Training Centre's administrative office for any reason. Paper records which need to be retained should be stored in the secure archiving cupboard until the date shown when destruction is allowed.

Privacy Notices

Privacy notices should be GDPR compliant and should be reviewed on an annual basis by the Centre Manager

Retention

Data retention is dictated by contractual requirements (see Appendix 2) and can be up to twelve years. Documents will be stored in secure storage should it be required for audit purposes. A disposal date must also be clearly marked and once this date is past the data should be disposed of as shown below.

Documents/electronic media containing personal data must not be disposed of along with general waste. Any hard copy documents/electronic media that are no longer required must be kept in a locked cabinet and put into secure shredding bins. Hard drives must be physically destroyed at the end of their serviceable life.

Training and Awareness

Training relating to data security and related issues will be featured in Team Briefing on 3 monthly basis.

ICO

Park Education and Training Centre is registered with the Information Commissioner under the terms of the Data Protection Act. Access to learner/clients and other third party information is restricted to the individual or organisation concerned and the relevant authorised staff. External access to this information is restricted to contractually or previously authorised organisations, and staff, learners, clients and other parties are given prior notice that such access may be required. External access is restricted to authorised personnel from funding bodies, Ofsted inspectors and awarding bodies, and access is restricted to only the information relevant to their purposes. Transmission of data to third parties is limited to that required to obtain the necessary funding for the learners'/clients' programs, according to the relevant funding contract. No data or information is passed to any other person or organisation without the specific permission of the learner, client or organisation being obtained.

Subject Access Requests

A subject access request applies to all personal data held by Park Education and Training Centre. If a subject request is made, it must be checked to ensure that the request is valid. The subject's identity must be verified prior to release of any information and reasonable measures must be taken to verify the identity of the data subject. Data must be provided within one calendar month. All subject access requests should be routed to the Centre Manager in the first instance. A log will be kept of any decisions (non-contractual) made.

Reviewed
May 2018

Appendix 1
Password Policy

Passwords must **not** be written down

Passwords must **not** be shared with other people

Passwords must meet the following minimum requirements:

- Not contain all or part of the user's account name • Be at least eight characters in length
- Contain characters from three of the following four categories:

  1. English uppercase characters (A through Z) 2. English lowercase characters (a through z)
  3. Base 10 digits (0 through 9)
  4. Non-alphabetic characters (for example, !, $, #, %)

If for any reason you cannot login to the network you must inform the Centre Manager who will reset your password.

Appendix 2
Retention Schedule

ESFA Data	12 years
ESF Data	12 years
Accounts/Payroll	6 year
Portfolio Data	Up to 3 years following completion/withdrawal