Guidance for Encryption of Multimedia Assessment Evidence

Guidance for centres with entries for Pearson BTEC and/or Pearson Edexcel qualifications in which recordings or images of candidates are sent to Pearson for assessment purposes.

Context
Changes to Data Protection legislation has led to a concern about the privacy of candidate data when sending work for assessment. This guidance has been written to help you understand how to protect this data.

Submission of candidate / learner evidence
This guidance applies to units where assessment evidence is submitted on multimedia devices, such as discs or USBs, in the form of either audio and/or visual recordings, or images of candidates. Other units, which do not involve images or recordings, can be sent in the usual way.

Method of postage
All packaging in which the candidate/learner work is submitted must be securely tied, sturdy and double wrapped to protect the materials.

We advise that work is despatched by tracked delivery. More detailed guidance for Pearson Edexcel centres can be found here. For Pearson BTEC externally assessed units, please refer to the information here.

- **Other specific methods of despatch for Pearson BTEC internal units**
  For BTEC internally assessed units, centres can take advantage of the paid for Parcelforce tracked service. There is also the option to submit units electronically for sampling via Dropbox, Google Classroom or Google Drive or to upload recordings onto a platform such as YouTube or Vimeo where they can be password protected. Folders or files can be shared with the allocated Standards Verifier until sampling has been completed; if these are password protected, the password should be sent in a separate email to the Standards Verifier.

- Internal assessment documentation can also be produced using myBTEC which removes the need for hard copies of these documents to be sent.

Encryption

To ensure that evidence of this nature remains secure, we recommend that you encrypt the media upon which it is saved.

In order for us to support encryption, we need to ensure that our appointed assessors can access it. For this reason, you must only submit material that can be viewed on VLC media player, QuickTime player and/or Windows media player.

Guidance on encryption of portable media:

1. **USB Removable Drive**

   Windows
   (This method only works for Windows versions with Bitlocker support if you use a version of Windows with no Bitlocker support use the zip method below and copy the zip file to USB)

a) Insert an empty USB drive.
b) Right-click the USB drive icon and select "**Turn On Bitlocker**" option.
c) Select "**Use a password to unlock the drive**" and enter and confirm a password.
d) Copy the data to the target USB drive.

   Mac

a) Insert an empty USB drive.
b) Right-click the USB drive icon and select the "**Encrypt**" option.
c) Enter and confirm a password.
d) Copy the data to the target USB drive.

2. **CD or DVD**

As it is not possible to directly encrypt a CD or DVD using common tools, this submission method will require you to create an encrypted compressed .zip file which should then be saved onto a CD or DVD. Third party software will be needed for this operation. Some examples are given below but other programmes are available.

   7-Zip
   These instructions are for the 7-Zip program which is free and open source software available from www.7-zip.org.

a) Open 7-Zip and browse to the data location on your drive (file or folder)
b) Click "**Add**" and in the Add to Archive window select archive format as "**zip**" and in the Encryption section enter and confirm a password.
c) The zip file will be created in the target location.

d) Create a CD or DVD containing just the zip file.

WinZip
These instructions are for the Winzip program which has a free evaluation version available from www.winzip.com

a) Open WinZip and in the actions pane change the slider option for Encrypt to "**on**"
b) Add data to the new zip file by dragging and dropping into Winzip
c) Enter a password when prompted and confirm.
d) Once all the required data is in the zip file then save the zip file.
e) Create a CD or DVD containing just the zip file

Letting us know
When you have encrypted your media, please despatch the physical evidence as per the instructions you have been given. **Do not** include the encryption password with the candidate/learner work.

The encryption password should instead be sent to one of the following email addresses:

Pearson BTEC External Assessments	btecngexams@pearson.com
Pearson BTEC Internal Assessments	svreports@pearson.com
Pearson Edexcel	courseworkmarks@pearson.com

Remember that you need to include your centre number, name and the unit/component details within your email. Please also let us know in the same email what type of computer the content was encrypted with (Mac or Windows).