Procedures for the Delivery of Password Tests – Users

These are English Language Testing Ltd's procedures for administering Password tests based on those used in Password Accredited Test Centres to ensure reliable and accurate results. This is particularly important when tests are to be used for high stakes purposes such as in making as admissions or employment decisions and in support of visa applications.

All Password test sessions shall be invigilated by staff of the organisation purchasing Password tests (the User) or of a contracted representative of the User in accordance with the Terms and Conditions for the use of the Password testing system agreed by the User. Password test invigilator(s) shall have been adequately trained in running Password tests and their invigilation by the User.

Any failure by the User or their contracted representatives to take all reasonable measures, either given in these procedures or otherwise, to protect validity of Password test results, the reputation of Password tests and the security of the Password test question and answer content may lead to suspension and/ or cancellation of the User's access codes to run Password tests.

Instructions for technical test delivery and equipment (computer hardware and software specifications, Internet connection etc.) are given in the latest "Instructions For Delivering Password XYZ Tests" where XYZ is the Password test type to be administered.

1   Physical Environment Standards

1.1   Rooms used for Password test sessions must adhere to the following minimum physical environment standards. Password tests rooms must:

- be enclosed and have opaque walls, with doors that are shut during a Password test session, and have no through traffic;

- have suitable lighting and be at a comfortable room temperature, be quiet, smoke-free, and have no external distractions;

- have facilities to enable the test taker(s) (candidate(s)) to take the Password test effectively; specifically, candidate(s) must have a flat surface on which the test computer display is placed and candidates must have a chair which is at a level for comfortable use of the display, keyboard and mouse;

- have displays spaced so that no candidate can see another's display EITHER at least 0.6m apart with privacy screening in place OR at least 1.2m apart;

- not present any candidate during a Password test with an opportunity to view or use any resources which may aid the candidate in answering the test (e.g. dictionaries, text books, notebooks, wall charts, another candidate's PC screen etc.);

- not have any facilities for the candidate to make notes of Password test content (such as pens and paper) save as allowed in Listening and Speaking Password test modules on

white boards which must not be kept by candidates as described in as described in the latest "Instructions for delivering the Password XYZ test").

1.2   The Password test room shall not be used for anything other than Password testing during the Password test session.

1.3   All Password test access codes shall be kept in a secure place.

2   Authentication Standards

2.1   The invigilator(s) must assure themselves that the candidate actually taking the Password test is the individual expected. The level of checking and identification documentation to be presented should be appropriate to the purpose of the Password test. For example, if the result is to be used to support a visa application, current valid Government issued photographic identification (passport, national identity card, military identity card) with a signature should be provided by the candidate. Documents must be originals not photocopies. However, for a Password test taken as an internal university test, a University student card may be sufficient and identity evidence retention deemed not necessary.

2.2   Invigilator(s) shall ensure that the candidate matches the photograph and signature of the identification document presented, is valid (i.e. not expired) and there is no evidence of tampering, especially with the photograph, name, signature and expiry date. The UK's Centre for the Protection of the National Infrastructure (CPNI) has an excellent identity document verification guide at www.cpni.gov.uk.

2.3   For each candidate invigilator(s) must (unless deemed by the User unnecessary) retain evidence on the candidate's identity:

  - take a high quality digital colour "passport" style photograph;

  - a sample of their signature;

  - make a high quality photocopy or scan of (at least) the photo page of the identity document presented.

This evidence must be safely stored and handled as determined appropriate by the User.

2.4   Invigilator(s) must ensure that there is no opportunity for candidates to be substituted in the entire Password test process from initial authentication until after the Password test session has been completed.

2.5   Invigilator(s) must check that the information entered by the candidate into the "candidates details" page at the start of the Password test are correct and match the identification presented before the candidate commences the test, and ensure that this is the same candidate that was previously checked.

2.6   If the Password test is split into two parts, if there has been any possibility of candidate substitution (e.g. there was a break period and candidate(s) allowed to leave the Password test room), identification documentation must be rechecked at the start of the second part of the Password test both against the candidate(s) and the previously captured information displayed on the Password test candidates details page.

3   Procedure Standards

3.1   Repeated taking of Password tests is not allowed. A candidate may normally take only one Password test in any twenty eight day period. In exceptional circumstances, such as illness during the first Password test, a second may be taken. An accurate record must be kept of the exceptional circumstances and supplied to ELT upon request. No candidate is allowed to take more than two Password tests within any twenty eight day period.

3.2   Candidate(s) shall be informed of identification document requirements before attending the Password test session.

3.3   No Password test shall be run during times that the User has been notified that system maintenance is taking place.

3.4   PCs to be used for Password testing shall be set up and checked as described in the latest "Instructions For Delivering Password XYZ Tests".

3.5   All electrical equipment belonging to candidate(s) including mobile phones shall be switched off. These and all other personal belongings (especially pens, paper, computers, tablets, mobile phones, memory sticks, cameras, video recorders, personal headphones and similar) shall be placed away from the test PC and kept safe in a separate room.

3.6   The Password test room shall be set up before candidate(s) enter with sufficient PCs and other equipment. The set up, including microphones and headphones if used, must be tested to be fully working and headphone volume set to a comfortable level. The test shall be accessed as described in the latest "Instructions For Delivering Password XYZ Tests" and left on the "Welcome" page when candidate(s) enter the room.

3.7   If allowed in " Instructions For Delivering Password XYZ Tests" for the Password test being taken (i.e. for Speaking and Listening test modules only), candidates should be issued with reusable white boards, dry wipe pens and erasers.

3.8   Invigilator(s) must brief candidates on the Password test they will take following the materials supplied by ELT and including the :

- Authentication Standards;

- Invigilation Standards;

- Procedure Standards;

- consequences if these Standards are breached by the candidate;

- how to fill in the Password test candidates details page;

- Password test structure, navigation and question formats,, breaks in a two part test and time allowed.

3.9   Upon completion of the Password test the invigilator(s) shall ensure the Password test has been completed and PCs shut down. Any headsets and white boards etc. must be collected for reuse and security reasons.

3.10   Candidates shall only be allowed to take away the personal belongings that they arrived with.

3.11   See the latest "Instructions For Delivering Password XYZ Tests" for information dealing with Internet connection loss during a Password test session.

3.12   The User and invigilator(s) shall not store or make copies of or notes on Password test content i.e. its questions and answer prompts in any way including but not limited to printing and use of recording devices whether electronic, software or "pen and paper". The User and invigilator(s) shall not coach candidates on Password test content in any way, and only use briefing and preparation materials authorised by English Language Testing Ltd.

4   Invigilation Standards

4.1   The invigilator(s)'s view of candidates shall be unobstructed, and invigilators shall monitor all candidates at all times, during the Password test session.

4.2   At most there shall be fifteen candidates per Password test invigilator.

4.3   Invigilator(s) shall not assist candidates in any way (unless the candidate is taking Password under authorised special needs assistance).

4.4   Invigilator(s) shall ensure that no visual, aural or other aids are available to the student during the Password test (unless the candidate is taking their Password test under authorised special needs assistance).

4.5   Invigilators(s) have a duty to actively watch and uphold the Invigilation Standards. They shall observe a respectful silence and their mobile phones shall be switched off.

4.6   Invigilator(s) must not involve themselves with any activity which may distract them from monitoring candidates (e.g. working on a PC or paper, and any candidate assistance which is only allowable as outlined below should be minimal).

4.7   During the Password test the Password test regulations shall be upheld:

- Candidate(s) must obey all instructions and directives given by an invigilator;

- there shall be no talking between candidates;

- there can be no use of dictionaries (paper or electronic) or other any other aids;

- use of electronic and data capture equipment of any kind is strictly forbidden (this includes but is not limited to pens, paper, computers, tablets, mobile phones, memory sticks, cameras, video recorders , personal headphones etc.);

- Candidate(s) cannot move around or leave the room nor attempt to look at each others' display or work;

- any candidate wishing to attract the invigilator(s)'s attention should remain silent, raise their hand and wait for the invigilator;

- Candidate(s) cannot ask the invigilator(s) any questions with the exception those regarding Password test navigation, the PCs or other Password test equipment;

- for avoidance of doubt the invigilator(s) shall not answer any questions regarding the content of the Password Test;

- if any candidate interaction or other activity could distract from the invigilator(s) observing the candidates or otherwise impede Password test invigilation, then the invigilator shall not involve him/herself in this;

- toilet breaks can only be permitted if there is a second invigilator to escort the candidate;

- at no point will the Password test timer be reset or paused;

- notes cannot be taken (save as allowed in Listening and Speaking Password test modules on white boards which must not be kept by candidates as described in as described in the latest "Instructions for delivering the Password XYZ test").

- no materials may be removed by candidates at the end of the Password test session.

4.8   If the candidate has their test interrupted (halted) the invigilator(s) must decide if this was accidental or an attempt to cheat. If the invigilator(s) judge that the interruption was accidental, the candidate may be allowed to restart the test. See the latest "Instructions For Delivering Password XYZ Tests" for more information on test interruption.

4.9   Grounds for disqualification of a candidate from completing a Password test include but are not limited to:

- failure to abide by the Password test regulations;

- failure to present suitable identity documents, presenting fraudulent identification documents or entering fraudulent information into a Password test;

- cheating, or attempting to cheat, in any way including repeated Password test interruption;

- use of personal items especially any that enable cheating including mobile phones;

- removal, or attempted removal, in any way of information on Password test content i.e. it's questions and answer prompts;

- assisting, or accepting assistance from, another candidate or invigilator in any way;

- disrupting the Password test session in any way;

- offering bribes in money or any other form to the User, invigilator(s) or others;

- threatening or intimidating in any way the User, invigilator(s) or others;

- attempting to take repeated Password tests.