

Procedures for the Delivery of Password Tests – Partners

(previously titled "Procedures for the Delivery of Password Tests – Users")

These are English Language Testing Ltd's (ELT's) Procedures for administering (delivering) secure Password tests by organisations purchasing these tests, also known as Password Partners or simply Partners. They are based on those developed for 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 admissions or employment decisions and in support of visa applications. They may be adapted by the Password Partner to suit their particular circumstances where this does not compromise the integrity of the Password test, or the Password testing or results.

These Procedures do not apply to Password tests branded Solo (for low stakes use), Distance Learning, Practice or Plus tests intended to be taken un-invigilated (un-proctored) "at home" by test takers (candidates) though Partners may well wish to use these as guidance for their regulations. Note that they apply (save for 3.4, 3.7, 3.8, 3.10, 3.11) to Solo tests when the test is used for high stakes purposes such as university admissions and visa support and the test is remotely invigilated.

All Password test sessions to which these Procedures apply shall be invigilated (in person or remotely) by staff of the Partner or of a contracted agent or representative or service provider (representatives) of the Partner (or for Plus test by ELT's contractor) in accordance with the "Terms And Conditions For The Use Of Password Tests" agreed by the Partner. Password test invigilator(s) shall have been properly trained in running Password tests and their invigilation by the Partner.

Any failure by the Partner or their 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 Partner's login and password 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. If the test is to be remotely invigilated, the candidate must provide suitable equipment to take the test, including a web camera or other device to allow monitoring and/ or recording during the test.

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; and
- have suitable lighting and be at a comfortable room temperature, be quiet, smoke-free, and have no external distractions; and
- have facilities to enable for the candidate(s) to take the Password test effectively; specifically, candidate(s) must have a flat surface on which the test computer display, keyboard and mouse are placed and candidates must have a chair which is at a level for comfortable use of the display, keyboard and mouse; and
- when there is more than one candidate 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; and
- 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.); and
- not have any facilities for the candidate to make notes (such as pens and paper) of Password test content (questions and answer options) save the white boards (which must not be kept by candidates) as allowed in Listening, Speaking and Maths Password test modules (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 logins and passwords 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 and outside their home country the candidate's passport should always be used. 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, the document is current (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, www.cpni.gov.uk) has some excellent resources to advise on identity document verification.

- 2.3 For each candidate invigilator(s) must (unless deemed by the Partner 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 page(s) with the name, date of birth, signature and photo of the identity document presented.

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

- 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 Administration Standards

- 3.1 Repeated taking of Password tests is not allowed. A candidate may take only two Password tests in any twenty eight day period. This second test is intended to cater for circumstances such as illness during the first Password test or as a "resit" when a candidate narrowly misses a score they require for some purpose. No candidate is allowed to take more than two Password tests within any twenty eight day period unless there are exceptional circumstances, and any third Password test within any twenty eight day period must be authorised by ELT in advance.
- 3.2 Candidate(s) shall be informed of identification document and other requirements before attending the Password test session.
- 3.3 No Password test shall be run during times that the Partner has been notified that maintenance is taking place on the Password Platform test delivery system.
- 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 Candidates shall wear a simple plain top such as a basic tee or sweat shirt (without a front opening, without buttons, zips or pockets, without a design) which extends down to at least the waist). Candidates shall not wear hats, caps or scarfs, and head coverings are permitted for religious reasons only.

- 3.6 All electrical equipment belonging to candidate(s) including mobile phones shall be switched off, and candidates shall empty all pockets in the clothing. All personal belongings (especially pens, paper, computers (including laptops), tablets, mobile phones, watches (including smart watches), items of jewellery, memory sticks, cameras, video recorders, personal headphones and similar) shall be placed away from the test PC and kept safe in a separate room.
- 3.7 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 normally left on the "Welcome" page when candidate(s) enter the room. For large testing sessions the candidates may enter the login and password codes as directed by the invigilator(s).
- 3.8 If allowed in "Instructions For Delivering Password XYZ Tests" for the Password test being taken (i.e. for Speaking, Listening and Maths test modules), candidates should be issued with reusable white boards, dry wipe pens and erasers.
- 3.9 Invigilator(s) must brief candidates on the Password test they will take following the materials supplied by ELT and including:
- Authentication Standards; and
 - Invigilation Standards; and
 - Administration Standards; and
 - consequences if these Standards are breached by the candidate; and
 - how to fill in the Password test candidates details page; and
 - Password test structure, navigation and question formats, breaks in a two part test and time allowed.
- 3.10 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 for security reasons.
- 3.11 Candidates shall only be allowed to take away the personal belongings with which they arrived.
- 3.12 See the latest "Instructions For Delivering Password XYZ Tests" for information dealing with Internet connection loss during a Password test session.
- 3.13 The Partner and their representatives 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 Partner and their representatives and invigilator(s) shall not coach candidates on Password test content in any way, and only use briefing and preparation materials authorised by ELT.
- 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 when invigilated “in person”, five when invigilated remotely.
- 4.3 Invigilator(s) shall not assist candidates in any way (unless the candidate is taking Password under authorised special needs assistance, in which case assistance shall be limited to that authorised).
- 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, in which case assistance shall be limited to that authorised).
- 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; and
 - there shall be no talking between candidates; and
 - there can be no use of dictionaries (paper or electronic) or other any other aids; and
 - 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.); and
 - Candidate(s) cannot move around or leave the room nor attempt to look at each others’ display or work; and
 - any candidate wishing to attract the invigilator(s)’s attention should remain silent, raise their hand and wait for the invigilator; and
 - Candidate(s) cannot ask the invigilator(s) any questions with the exception those regarding Password test navigation, the PCs or other Password test equipment; and
 - for avoidance of doubt the invigilator(s) shall not answer any questions regarding the content of the Password Test; and
 - 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; and
 - toilet breaks can only be permitted if there is a second invigilator to escort the candidate; and
 - at no point will the Password test timer be reset or paused; and
 - notes cannot be taken (save as allowed in Listening, Speaking and Maths Password test modules on white boards which must not be kept by candidates 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 should be allowed to continue the test. See the latest "Instructions For Delivering Password XYZ Tests" for more information on test interruption.
- 4.9 When tests are invigilated remotely, remote invigilator's shall use suitable software and/ or other methods to both monitor the candidate behaviour and their PC screen, and candidates must have a suitable PC and web camera or other device. Prior to starting the test the remote invigilator shall:
- inform the candidate that they will be monitored throughout the test and that they may be recorded; and
 - ask the candidate to present their identity document to the web camera, and the invigilator should check (at least) that the photograph and name match that of the candidate, it is current, and appears not to have been tampered with; and
 - ask the candidate to confirm their full name and date of birth, and some questions based on information known to the invigilator from sources such as application forms or personal statements (the intention is to reinforce the identity document check); and
 - ask the candidate to use the web camera to scan the room for people (they must be alone) and potential aids to taking the test; the desk/ table being used must be clear of any objects except the test PC, the scan must include under and behind the desk and check that the door to the room is closed; and
 - check the PC setup (operating system and browser version etc.), single screen (no second monitor), no apps/ programs are running except for the test browser tab to be used to take the test and the monitoring software, that the Internet bandwidth is sufficient and the connection stable, and the headphones & microphone if being used are working; and
 - make the browser tab "full screen" if not already so, navigate to (or guide the candidate to) the Password Platform test login page and enter the test login and password; and
 - check that the information entered by the candidate into the "candidates details" page is correct and matches the identification presented.

- 4.10 Grounds for disqualification of a candidate from completing a Password test and/ or receiving a test result include but are not limited to:
- failure to abide by the Password test regulations; and
 - failure to present suitable identity documents, presenting fraudulent identification documents or entering fraudulent information into a Password test; and
 - cheating, or attempting to cheat, in any way including repeated Password test interruption; and
 - use of items especially any that enable cheating including mobile phones; and
 - removal, or attempted removal, in any way of information on Password test content i.e. it's questions and answer prompts; and
 - assisting, or accepting assistance from, another person in any way; and
 - disrupting the Password test session in any way; and
 - offering bribes in money or any other form to the Partner and their representatives, invigilator(s) or others; and
 - threatening or intimidating in any way the Partner and their representatives, invigilator(s) or others; and
 - attempting to take repeated Password tests beyond those allowed.

5 Other Procedures

- 5.1 For information on retakes (retaking a module of a test again because technical difficulties were encountered while taking a module) and resits (taking another complete test) see the latest "Password Tests – Resits And Retakes Procedures" document.
- 5.2 To request a correction to a candidate's details that were entered incorrectly into a test please contact ELT's Password support team for a "Password test candidate details correction request" form. This must be done as soon as possible after the testing date and evidence of identity may be required.
- 5.3 To request special needs accommodations that may be possible for candidates please contact ELT's Password support team for a "Password test candidate accommodation for special needs request" form. This must be done as long as possible in advance (at least one month is recommended) of the desired testing date. A fee may be charged and medical evidence may be required.