Data Security Policy

PAS has an obligation to keep information 'safe and secure' and have appropriate measures in place to prevent unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction in compliance with the GDPR. It is imperative, therefore, that we have security measures and policies in place to ensure that only those staff members with a business need to access a particular set of personal or sensitive data are allowed to access that data.

This PAS Security Policy sets out who can access the various types of personal data in PAS, the procedures for handling personal data and for ensuring the security of personal data (both manual files and on IT systems). It also contains procedures for the transmission of data to other parties.

The implementation of this Policy is subject to audit by a staff member nominated by the Data Protection Officer and may also be the subject of an internal audit investigation and report to the Audit Committee at any stage.

Access

Staff in Recruitment and Selection Units have access to personal data in respect of candidates for competitions and prospective board members. This data must only be used for the purposes of progressing a recruitment competition and must not be released outside of the organisation, or to anyone inside the organisation who is not involved in that particular recruitment competition, without permission from a senior manager.

Staff in support areas have access to personal information on staff members (HR and Finance Unit), candidates (IT), board members/assessors/invigilators (IT, Finance Unit and Recruitment Support) and suppliers (Recruitment Support and Finance Unit). This data must only be used for the purposes for which it was collected (contained in the relevant privacy notice) and must not be released outside of the organisation, or to anyone inside the organisation who does not have a legitimate reason for possessing the data, without permission from a senior manager. All staff in HR/CDU must sign a Confidentiality Statement.

Procedures for Handling Personal Data (Manual Files and on IT systems)

It is important that all personal data in PAS is used only for the purposes for which it was obtained and is kept confidential in PAS.

The following IT security measures are also in place and these procedures must be complied with:

(i) The Information Security Policy should be complied with at all times. PAS IT enforce a policy that requires a complex password for access to the corporate network. PAS have implemented a centrally controlled policy to force staff to change their network passwords regularly. The sharing of a user's individual network credentials is prohibited. Staff are required to lock or log off their pc when leaving their desk unattended – all computers are set to lock automatically after 5 minutes. Emails should be checked before sending to ensure they are addressed to the intended recipient.

(ii) Staff are required to ensure personal or confidential information is not displayed on computer screens in public areas of the office.

(iii) All personal and sensitive data held electronically is stored centrally. Access to both IT and Data Centre (hosts hardware and software on which personal data is stored) is restricted to staff in IT unit (swipe card required with IT access); access records and procedures are reviewed by senior management regularly.

(iv) PCs are disposed of securely using a specialist company; the hard drives shredded.

(v) The permissions of shared drives are regularly reviewed and restricted where appropriate (e.g. staff that have moved units will have their permissions changed) (it is the responsibility of the Line Manager to notify IT of any staff changes and to request access rights be changed).

(vi) Remote access is only permitted through a secure encrypted channel using two factor authentication (*see paragraph below*).

(vii) Anti-virus and anti-spyware software is installed on all personal computers and laptops.

(viii) Corporate firewalls are in place to prevent unauthorised access to office network.

(ix) All computers and servers are regularly and centrally patched against latest known vulnerabilities.

(x) Access to systems which are no longer in active use and which contain personal data is removed where such access is no longer necessary or cannot be justified.

(xi) Staff members who retire, resign or transfer from PAS will be removed immediately from mailing lists and access control lists. Relevant changes will also occur when staff are transferred to other assignments internally;

(xii) Personal or sensitive data held on applications and databases with relevant security and access controls in place (e.g. STAR) can only be copied to personal productivity software (such as word processing applications, spreadsheets, etc.) if it is copied into a directory to which only those working on a particular competition have access; this will be subject to audit and breaches may lead to actions under the Disciplinary Code;

(xiii) As part of the office's move towards paperless boards, tablets may now be used for selection boards. This means that applications may be temporarily stored on ShareFile in preparation for the board meeting. The tablets must be stored securely in PAS, and when being issued to board members, the relevant unit must ensure that the tablet is received only by the person for which it was intended. The unit must also ensure that all tablets are returned to IT after the relevant board meeting and that the board member has logged out; expiration dates for board data must be set on ShareFile;

(xiv) Other than as set out in (xiii) above, personal data must never be copied to portable storage devices, such as laptops, memory sticks, etc. that may be stolen or lost; the following also apply to the use of portable storage devises:

a. Personal, private, sensitive or confidential data must never be stored on portable devices. With regard to laptops, full disk encryption must be employed regardless of the type of data stored; staff are encouraged to exercise caution when accessing public Wi-Fi networks. No confidential or sensitive corporate information should be accessed or transmitted over an unsecured public Wi-Fi network.
b. passwords are enforced on smart phones and mobile devices and passwords used should be strong and secure as stated in the Information Security Policy;
c. When portable computing devices or mobile phones are being used in public places, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons;
d. Each device is authorised for use by a specific named individual and responsibility for the physical safeguarding of the device will then rest with that individual;
e. Laptops must be physically secured if left in the office overnight; when out of the office, the device should be kept secure at all times;
f. portable devices should never be left in an unattended vehicle;
g. all mobile laptops are regularly called in for AV updates and patches (immediate compliance with this is required) and all have full disk encryption; USB devices are centrally controlled and restrictions are in place in relation to the use of USB devices; USBs are only used for non-confidential and non-personal information, e.g. public presentations).

Remote Access

When accessing this data remotely, it must be done via a secure encrypted link.
Staff are expected to comply with this Code when accessing data remotely. If this involves downloading personal data on to your machine, you must save the completed document on the network and delete any information stored on your machine when you have completed your work. You must only use a machine (desktop PC, laptop, mobile phone or PDA) which is configured appropriately to PAS standards (e.g. with up-to-date anti-virus and anti-spyware software, full encryption, etc.) when remotely accessing centrally held personal or sensitive data. All wireless technologies/networks used when accessing PAS systems must be encrypted to the strongest standard available.

The above directions also apply to PAS Board Members or IT support consultants (if applicable and with appropriate permission) when accessing PAS systems remotely.

Appropriate Access and Audit Trail Monitoring

In order to capture instances of inappropriate access (whether internal or external), addition, deletion and editing of data, audit trails will be used as part of STAR.

The following procedures must be adopted in relation to manual records/paper files:

- ◊ Board members must be asked to sign a "Confidentiality Statement" and must be briefed by the PAS Representative on the requirement for confidentiality at all stages of the process. Assessors/Invigilators must also be asked to sign a "Confidentiality Statement" and be briefed by the relevant recruitment unit on the requirement for confidentiality.
- ◊ Care must be taken to ensure that candidates and selection board members calling at reception are not allowed to view personal data on other candidates/other boards (this includes the names of other candidates) so care should be taken with the board folders to ensure they cannot be accessed and care should be taken when checking candidates in that they cannot view information on other candidates (ensure they only receive a copy of their own application form).
- ◊ All board papers must be taken from the board room when the board is finished and the room must be locked if board papers are left unattended in the room at any stage.
- ◊ All board room keys must be handed into reception and the press where the keys are stored should be locked at all stages that reception is unattended (e.g. overnight) and the key to that press must be stored in a secure location.

- ◊ Care must be taken that candidates signing-in at test venues are not allowed to view personal data on other candidates (including names).
- ◊ Personal information which is being destroyed (e.g. copies of application forms following shortlisting/interviews) should be placed in the Confidential Waste Bin only. It will then be shredded in-house or externally by a contractor who has in his/her contract agreed to the office's data protection procedures and ensure that the confidentiality of all personal data is protected.
- ◊ When photocopying personal information (e.g.) application forms care should be taken to ensure all copies are removed from the photocopying room.
- ◊ Personal and sensitive information must be locked away when not in use or at end of day (e.g. application forms, order-of-merits, confidential reports, etc.).
- ◊ Access to paper records and files containing personal data is restricted only to those staff with business reasons to access them (files are stored off-site in secure storage when not in use; files in use are stored in the section to which they relate). Requests for files stored off-site are sent to Business Support Unit and the person to whom the file is released is recorded.
- ◊ Access to files containing personal data will be monitored by supervisors on an ongoing basis and is also subject to audit at any stage.

The following procedures must be adopted for sending personal information outside of PAS:

- ◊ Personal information should not be sent to other external parties unless it is absolutely necessary and complies with the General Data Protection Regulation, you must check with a senior manager before sending any personal information to persons outside of PAS.
- ◊ Personal information should not be sent by email unless it is encrypted and customers should be informed that they should not send in personal information by email; the disclaimer at the bottom of office emails advises customers of this*[1].
- ◊ The fax must never be used for transmitting documents containing personal data.
- ◊ You should ensure that the data will be delivered only to the person to whom it is addressed or someone acting on their behalf and that all of the documents are returned and when no longer required are disposed of in the confidential waste.

1

If data is being sent via standard email to an individual there should be a clear understanding and acceptance by the recipient of the risk involved in transmitting personal and sensitive data using this technology. There is a statement on our website that personal and sensitive data should not be sent to us by email.

- ◊ Internal post must be delivered only to the person to who it is addressed or to their manager if they are absent.
- ◊ If a request is received from another organisation for access to personal data, you must consult a senior manager who will decide whether releasing the information is justified and would be accepted under the terms of the GDPR. The senior manager will consult the Data Protection Officer for advice if necessary.
- ◊ Contractors, consultants and external service providers (including on-line test providers) contracted by PAS will be subject to strict procedures with regard to accessing personal data by way of formal contract in line with the provisions of the GDPR. The terms of the contract and undertakings given are subject to review and audit to ensure compliance.

Transfers of data should take place only where absolutely necessary, using the most secure channel available. To support this, PAS staff should adhere to the following:

- ◊ Data transfers should, where possible, only take place via secure on-line channels where the data is encrypted;
- ◊ Manual data transfers using removable physical media (e.g. memory sticks, CDs, tape, etc.) should not take place; if a senior manager decides that this must take place the data must be encrypted using the strongest possible encryption method available. Strong passwords/passphrases must be used to encrypt/decrypt the data; any such encrypted media should wherever possible be accompanied by a member of staff, be delivered directly to, and be signed for by, the intended recipient. Care should be taken to ensure that the password is sent securely to the intended recipient and that it is not disclosed to any other person; if the data is being sent by registered post/courier there should be a clear understanding and acceptance by both senders and recipients of the risk involved in transmitting personal and sensitive data using this technology.
- ◊ When a data transfer with a third party is required (including to/from other Government Departments/Offices and with on-line test providers), a written agreement should be put in advance of any data transfer. Such an agreement should define, where required: -
    - (i) the information that is required by the third party (the purposes for which the information can be used should also be defined if the recipient party is carrying out processing on behalf of PAS);
    - (ii) named contacts in each organisation responsible for the data;
    - (iii) the frequency of the proposed transfers;
    - (iv) an explanation of the requirement for the information/data transfer;
    - (v) the transfer method that will be used (e.g. Secure FTP, Secure email, etc.);
    - (vi) the encryption method that will be used;

(vii) the acknowledgement procedures on receipt of the data;

(viii) the length of time the information will be retained by the third party;

(ix) confirmation from the third party that the information will be handled to the same level of controls that PAS applies to the information;

(x) confirmation as to the point at which the third party will take over responsibility for protecting the data (e.g. on confirmed receipt of the data);

(xi) the method of secure disposal of the transfer media and the timeline for disposal;

(xii) the method for highlighting breaches in the transfer process;

(xiii) for data controller to data controller transfers (as opposed to a data controller to a data processor transfer), it needs to be clear that only necessary data is transferred to meet the purposes;

(xiv) clarification must be obtained in advance from the Data Protection Officer that such transfers are legal, justifiable and that only necessary data is transferred to meet the purposes;

(xv) particular attention should be focussed on data made available to third party data processors under contract for testing purposes. Live data should not be used for this purpose.

Staff, board members, assessors and invigilators are also instructed not to speak about confidential information in public or to mention PAS or any PAS related data when using social media.