INFORMATION SECURITY POLICY

Statement of policy

1. HM Academy t/a HM Tutors (the **Employer**, **we** or **our**) is committed to the highest standards of information security and treats data security and confidentiality extremely seriously.

2. This policy and the rules contained in it apply to all staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, temporary and agency workers, trainees, casual and fixed-term staff, apprentices, interns and any volunteers (**Staff** or **you**).

3. All Staff must familiarise themselves with this policy and comply with its terms.

Purpose of policy

4. In relation to personal data, under the UK General Data Protection Regulation (the **UK GDPR**), the Employer must:

   a. ensure the security of personal data, including protection against any unlawful or unauthorised data processing and accidental loss, damage or destruction, by utilising appropriate technical or organisational measures;

   b. demonstrate the consideration and integration of data compliance measures into the Employer's data processing activities, by implementing appropriate technical or organisational measures; and

   c. be able to demonstrate the use and implementation of such appropriate technical or organisational measures.

5. The purpose of this policy is to:

   a. protect against any potential breaches of confidentiality;

   b. protect the Employer's informational assets and IT systems and facilities against any loss, damage or misuse;

   c. supplement the Employer's Data Protection and Security Policy in ensuring that Staff are aware of and comply with UK laws and the Employer's policies and procedures on the processing of personal data; and

   d. raise awareness of and clarify the responsibilities and duties of Staff in respect of information security, data security and confidentiality.

6. This is a statement of policy only and does not form part of your contract of employment. The Employer may amend this policy at any time, in our absolute discretion, and we will do so in accordance with our data protection and other obligations. A new copy of the policy will be circulated whenever it is changed.

7. For the purposes of this policy:

   a. **Business Information** means any of the Employer's business-related information other than personal data about customers, clients, suppliers and other business contacts;

   b. **Confidential Information** means any trade secrets or other confidential information (belonging to the Employer or third parties) processed by the Employer;

   c. **Personal Data** means any information that relates to an individual who can be identified from that information, either directly or indirectly; and

   d. **Sensitive Personal Data** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), health, sex life, sexual orientation, genetic information or biometric information (where this is used to identify an individual).

Roles and responsibilities

8. All Staff have a responsibility for information security. The Employer's Data Protection Officer (DPO) has overall responsibility for this policy. Specifically, they must:

   a. implement and maintain this policy;

   b. monitor potential and actual security breaches;

   c. ensure Staff are aware of their responsibilities in relation to information security and confidentiality; and

   d. ensure compliance with the UK GDPR and all other relevant legislation and guidance.

Scope of this policy

9. This policy covers all written, verbal and digital information held, used or transmitted by or on behalf of the Employer, irrespective of media. This includes, but is not limited to:

a. paper records;

b. hand-held devices;

c. telephones;

d. information stored on computer systems; and

e. information passed on verbally.

10. The information covered by this policy may include:

a. Personal Data relating to Staff, customers, clients or suppliers;

b. other Business Information; and

c. Confidential Information.

11. This policy supplements the Employer's Data Protection and Security Policy and other policies relating to data protection, internet, email and communications, and document retention, including the Employer's:

a. Employee Privacy Notice.

The content of these policies must be considered and taken into account alongside this policy.

General principles

12. All information must be:

a. treated as commercially valuable; and

b. protected from loss, theft, misuse or inappropriate access or disclosure.

13. Through the use of appropriate technical and organisational measures all Personal Data, including Sensitive Personal Data, must be protected against:

a. unauthorised and/or unlawful processing; and

b. accidental loss, destruction or damage.

14. Staff and line managers should discuss what security measures (including technical and organisational measures) are appropriate and which exist to protect any information accessed by Staff in the course of employment.

15. Any information, apart from Personal Data, is owned by the Employer and not by an individual or team.

16. Any information must only be used in connection with work being undertaken for the Employer. It must not be used for any other personal or commercial purposes.

17. Any Personal Data must only be processed for the specified, explicit and legitimate purpose for which it is collected.

Information management

18. Any Personal Data must be processed in accordance with:

a. the data protection principles;

b. the Employer's policies on data protection generally (including the Data Protection and Security Policy); and

c. the Employer's other relevant policies.

19. All Personal Data collected, used and stored must be:

a. adequate, relevant and limited to what is necessary for the relevant purposes; and

b. kept accurate and up to date.

20. The Employer will take appropriate technical and organisational measures to ensure that Personal Data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage. These measures include:

a. The encryption of Personal Data.

b. Strictly limited access rights to certain datasets to ensure only those authorised to process Personal Data have access. .

c. Two factor lock system .

21. Any Personal Data and Confidential Information must not be kept any longer than is necessary and will be stored and destroyed in accordance with our policies on data retention.

Human resources (HR) information

22. Due to the internal confidentiality of personnel files, access to these files and any information contained therein is limited to the HR Department. Non-HR Staff are not authorised to access HR information, except as provided for in any individual roles.

23. Personnel information must also be kept strictly confidential by any Staff involved in:

a. the recruitment process;

b. a management role; or

c. a supervisory role.

24. Under the UK GDPR and other relevant legislation, Staff may ask to see their personnel files and obtain access to any other Personal Data about them.

Access to offices and information

25. All office doors, office keys and access codes must, at all times, be kept secure. Office keys and access codes must at no time be given to or communicated to any third parties.

26. All documents containing and any equipment displaying Confidential Information should be placed and positioned so that anyone passing by cannot see them (e.g. through office windows or glass doors).

27. Any visitors must:

a. sign it at reception;

b. be accompanied by Staff at all times; and

c. not be left alone in areas or situations where they may have access to Confidential Information.

28. Meetings with visitors must, where possible, take place in meeting rooms. If a visitor meeting takes place outside a meeting room, in an office or other room containing Employer information, steps must be taken to ensure no Confidential Information is visible and accessible to the visitors.

29. All paper documents, backup systems and devices containing Confidential Information must be securely locked away:

a. whenever desks are unoccupied; and

b. at the end of the working day.

Computers and IT

30. Where available on our systems, password protection and encryption must be used to maintain confidentiality.

31. All computers and other electronic devices must be password protected. Such passwords must be changed regularly and must not be recorded anywhere (e.g. written down) or made available to others.

32. To minimise the risk of accidental loss or disclosure, all computers and other electronic devices must be locked when not in use, including when left unattended at a desk.

33. All data held electronically must be securely backed up as soon as possible in accordance with the Employer's internal backup procedure.

34. Confidential Information must not be copied onto removable hard drives, CDs or DVDs, floppy disks or memory sticks, without the express permission of the IT Department. Any Personal Data held on such devices must, as soon as possible, be transferred to the Employer's computer network to be backed up and then deleted from the device.

35. Staff must:

a. ensure that they do not introduce viruses, malware or malicious codes onto the Employer's systems.

b. not install or download from the internet any software without it first being checked for viruses.

Staff should speak to the IT Department for more information and guidance on appropriate steps to be taken to ensure compliance.

Communications and transfer of information

36. When speaking in public places (e.g. when speaking on a mobile phone), Staff must take care in maintaining confidentiality.

37. Confidential Information must be marked 'strictly private and confidential' and circulated only to those who need to know the information in the course of their work

38. Confidential Information must not be removed from the Employer's offices (and systems) unless required for authorised business purposes, and then only in accordance with the subsequent paragraph.

39. If the removal of Confidential Information from the Employer's offices is permitted, all reasonable steps must be taken to maintain the confidentiality and integrity of the information. This includes, but is not limited to, Staff ensuring that Confidential Information is:

a. stored with strong password protection, which is kept locked when not in use;

b. not transported in see-through or other unsecured bags or cases, when in paper copy;

c. not read in public places when working remotely (e.g. in waiting rooms or on trains); and

d. not left unattended or in any place where it is at risk (e.g. in airports or conference centres).

40. Care must be taken to verify all postal and email addresses before any information is sent to them. Particular care must be taken when checking and verifying email addresses where auto-complete features may have inserted incorrect email addresses.

41. Before being sent by email or recorded delivery, all sensitive or particularly confidential information should be encrypted.

Personal email and cloud storage accounts

42. Personal email accounts (e.g. Google, Hotmail and Yahoo) and cloud storage services (e.g. Google Drive, iCloud and OneDrive) are vulnerable to hacking and do not provide the same level of security as the services provided by the Employer's IT systems.

43. Staff must not use personal email accounts or cloud storage accounts for work purposes.

44. If large amounts of data need to be transferred, Staff should speak to the IT Department.

Working from home

45. Unless required for authorised business purposes, and then only in accordance with the subsequent paragraph, Staff must not take information home with them.

46. Where information is permitted to be taken home, Staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular, all Confidential Information and Personal Data must be:

a. kept in a secure and locked location, where it cannot be accessed by others (including family members and guests); and

b. retained and disposed of in accordance with paragraph 21 above.

47. Staff must not store any Confidential Information on their home computers or other devices (e.g. laptops, PCs or tablets).

Transfer to third parties

48. Third party service providers should only be engaged to process information where appropriate written agreements are in place to ensure that they offer appropriate data protection, confidentiality and information security protections and undertakings. Care must be taken to consider whether any such third party service providers will be considered data processors for the purpose of the UK GDPR.

49. Staff involved in the process of setting up new arrangements or altering existing arrangements with third parties should speak to and consult with the DPO for more information and guidance.

International data transfers

50. There are restrictions on (onward) transfers of Personal Data to international organisations outside of the UK. Staff may not transfer Personal Data outside the UK (including to international organisations outside the UK).

51. For more information, see the Employer's Data Protection and Security Policy available from the DPO. If you have any questions or concerns please contact the DPO or Legal Department.

Training

52. The Employer will provide training on the concepts and measures contained in this policy to all Staff as part of the induction process and at regular intervals thereafter or whenever there is a substantial change in the law or our policies and procedures.

53. Training is provided online. The completion of such training is compulsory. The Employer will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or this policy, please contact the DPO.

Reporting data breaches

54. All Staff are under an obligation to report actual or potential data protection compliance breaches to enable the Employer to:

a. investigate the breach and take any necessary remedial actions;

b. maintain a register of compliance breaches; and

c. make any applicable notifications (e.g. to the Information Commissioner's Office).

55. For more information on the Employer's reporting procedure, contact the DPO.

Consequences of non-compliance

56. The Employer takes compliance with this policy very seriously and failure to comply with this policy puts Staff and the Employer alike at significant risk.

57. Due to the importance of this policy, failure to comply with any of its procedures and requirements may result in disciplinary action and dismissal.

58. If you have any questions or concerns about anything in this policy, please contact the DPO at info@hmtutors.co.uk.

Attribution

59. This Information Security Policy was created using a document from Rocket Lawyer (https://www.rocketlawyer.com/gb/en).