Glaston Hall, Spring Lane, Glaston, Rutland LE15 9BX Telephone: 01572 821985 Facsimile: 01572 820565
Email: info@manaeducation.co.uk www.manaeducation.co.uk

# Data Protection Policy

***Scope of this policy***

Mana needs to comply with the Data Protection Act 1998 in relation to all personal data. To ensure this happens, it has developed this policy which sets out the obligations of staff in this respect.

This policy and the Data Protection Act apply to all personal data handled by the University, both that held in paper files and data held electronically. So long as the processing of the data is carried out for Company purposes, it also applies regardless of where data is held, (for example, it covers data held in the office and on mobile devices such as on electronic notebooks or laptops) and regardless of who owns the PC/device on which it is stored.

'Processing' data is widely defined and includes every plausible form of action that could be taken in relation to the data such as obtaining, recording, keeping, or using it in any way; sharing or disclosing it; erasing and destroying it.

***Definitions***

**Personal data**

Data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller. Mana is the data controller.

Examples of personal data are the name and address of an individual or a candidate which when put with other information held by Mana could identify a candidate, staff member or client. The majority of staff (including all line managers) will therefore handle personal data at least occasionally.

**Sensitive personal data**

Personal data consisting of information relating to:

- race or ethnic origin of the data subject
- their political opinions
- their religious beliefs or other beliefs of a similar nature
- whether they are a member of a trade union
- their physical or mental health or condition
- their sexual life
- any commission or alleged commission by them of any offence
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

**Confidential data**

Data given in confidence or data agreed to be kept confidential, in other words a secret between two parties, and that is not in the public domain.

Some confidential data will also be personal data and/or sensitive personal data and therefore come within the terms of this policy. Staff working in certain functions and in senior management roles will handle confidential data regularly.

Mana also handles research data which comprises materials collected or created for the purposes of analysis to generate original research results. Some research data will contain personal data and/or sensitive personal data and in all such cases the provisions of this policy apply.

***Legal framework***

Mana needs to collect and keep certain types of information about the people with whom it deals. This includes information relating to its staff, students and other individuals. It needs to process 'personal data' for a variety of reasons, such as to recruit and pay its staff, to record the academic progress of its students and to comply with statutory obligations (for example, health & safety requirements).

The Data Protection Act 1998 applies to all 'personal data' processed by Mana and to comply with the law, all personal data must be collected and used fairly, stored safely and not disclosed to any third party unlawfully.

***Responsibilities of staff***

All staff must:

1. Be mindful of the fact that individuals have the right to see their 'personal data' (and this may include for example information received from prospective students or staff written in connection with an application to Mana or any comments written about them in emails). They should not therefore record comments or other data about individuals which they would not be comfortable in the individual seeing, either in emails or elsewhere.
2. Immediately report the matter to their line manager and bring it to the attention, if they find any lost or discarded data which they believe contains personal data, (for example, may include a memory stick).
3. Immediately report the matter to their line manager and bring it to the managers attention, if they become aware that personal data has been accidentally lost or stolen or inadvertently disclosed (for example, if their laptop is stolen or their phone is lost and it has personal data stored on it),
4. Hold the contents of any personal data which comes into their possession securely.
5. Ensure that any personal data they provide to Mana (for example, their contact details) is accurate.
6. Notify Mana promptly of any changes to their personal data (for example, change of address or emergency contact details).
7. Only ever obtain or use personal data relating to third parties for approved work or study-related purposes.

Staff and students with access to 'personal data' must:

1. Ensure that they only ever process personal data in accordance with requirements of the Data Protection Act 1998 and in particular follow the 8 Principles it contains. The best way to ensure compliance is through familiarisation with this policy and the guidance we provide. Key points insofar as compliance is concerned include:
    - Fair processing – for example, ensure that the individual consents to their data being used and knows what it will be used for, and ensure that it is not subsequently used for something else

- Data Security – ensure any personal data which is held is always kept and disposed of securely, (taking into account any cyber security considerations).
- Non-disclosure – ensure personal data is not disclosed to any authorised third party.

2. If they are going to be working remotely or using a mobile device to store data (for example, a laptop, tablet or mobile phone), it is vital that they are familiar with our Remote Working & Use of Mobile Devices Guidance, detailed below as special considerations apply.
3. Be mindful of the scope of Data Protection regulation. This includes that fact that 'personal data' is widely defined, (and so will cover for example comments made about an individual in an email to someone else), and the fact that it covers data held on remote devices (such as tablets and on mobile phones) regardless of who owns the actual device and where the device is stored.
4. Seek advice whenever a new or novel form of processing personal data is contemplated or if any data protection related concerns ever arise.

***Data Protection Act principles***

Anyone using personal data must comply with the 8 Data Protection Principles contained in the Data Protection Act 1998 as they define how person data can be legally processed: In summary these state that personal data shall:

1. Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. Be adequate, relevant and not excessive for those purposes.
4. Be accurate and kept up to date.
5. Not be kept for any longer than is necessary.
6. Be processed in accordance with the data subject's rights.
7. Be kept safe from unauthorised access, accidental loss or destruction.
8. Not be transferred to a country outside the European Economic Area (unless that country has equivalent levels of protection for personal data).

***Data security***

Keeping personal data properly secure is key in complying with the Data Protection Act. All staff are therefore responsible for ensuring that if they keep any personal data, it is kept securely and is not disclosed (either orally or in writing or accidentally) to any unauthorised third party.

**Keeping personal data secure**

This includes, as a minimum:

1. Ensuring that any personal data recorded in paper form or hard copy documents are kept in locked filing cabinets or locked drawers or in locked offices.
2. Ensuring that the same measures are taken in regards to any discs or memory sticks or similar devices on which personal data is held, for example, they must also be kept in a secure and locked location.
3. Ensure that if any personal data is held on a Mobile Device that it is properly password protected and where appropriate encrypted.
4. Ensuring special care is taken whenever data is transferred from one place to another to ensure security of the data is paramount, (for example, to avoid losing memory sticks in transit or to avoid sensitive personal data being transferred to a PC which is not password protected and encrypted).

***Prohibited activities***

The following activities are strictly prohibited:

- using data obtained for one purpose for another supplemental purpose (for example, using contact details provided for HR-related purposes for marketing purposes)
- disclosing personal data to a third person outside of Mana without the consent of the data subject.

***Rights to access information***

Individuals have the right to access any personal data that relates to them which Mana holds. Any person who wishes to exercise this right should speak to a senior manager for details of how to do so.

***Implications of breaching this policy***

It is a condition of employment in the case of staff that they will abide by the policies and rules of the Company. Any breach of this policy will be considered to be a disciplinary offence and may lead to disciplinary action. A serious breach of the Data Protection Act may also result in Mana and/or the individual being held liable in law.

***Conclusion***

Compliance with the Data Protection Act 1998 is the responsibility of all members of the Company. Any questions about this policy or any queries concerning data protection matters should be raised with the Senior Managers.