Data protection Policy

1. Policy Statement

1.1. Winsor Education is committed to abiding by the Data Protection Act 1998 ('The Act') & the GDPR and also commits to the observation of the act execution at the institute.

2. Purpose and Aim

2.1. The purpose and aim of this policy is to establish clear college guidance for all employees / departments on their role and responsibility in the implementation and compliance of 'The Act'.

3. Key Principles

3.1. Winsor Education is committed to ensuring that all the policies and procedures are understood and implemented by all staff members at all times.

3.2. The staff is recommended to read the ICO's Guide to Data Protection.

3.3. The policy covers the implementation of the data protection principles in the following areas.

3.3.1. Acquisition of data

3.3.2. Storage and safeguarding of the data

3.3.3. Processing of the data

3.3.4. Disclosure of the data

3.3.5. Transfer of the data

3.3.6. Destruction of the Data

It is our policy to ensure that:

3.4. The College staff abides by their responsibility in relation to The Act.

3.5. The staff reads and understands this policy.

3.6. The staff understands the meaning of sensitive / personal data.

3.7. The staff conforms to the expected standards in relation to the system and the use and safeguarding of any personal data.

3.8. The staff contacts the senior management in case of any doubts; the staff should not risk rights of any individual.

Data protection Principles

3.9. The personal data is processed fairly and lawfully.

3.10. The personal data should only be obtained for lawful purposes.

3.11. The personal data should be kept accurately and where necessary, kept up to date.

3.12. The personal data should be kept in secure filing cabinets and password protected computers, which should be locked if the designated person is away from their area.

3.13. The personal data should not be transferred or transmitted to any country outside of the EEA unless for lawful reasons and provided that the country abides by a data protection policy and shows an adequate level of adherence to the protection of personal data.

3.14. The personal data may be disclosed to reliable organisations such as Home Office, Government bodies, inspection bodies and certificate awarding institution etc. Approval must be sought from the senior management prior to disclosure of the data.

3.15. The data may be kept as long as required and then the destruction of the data can take place in such a way that traces of personal information are not visible to any third party. Preferably a shredder must be used for the destruction of paper based data and the electronic data must be destroyed on an offline computer with no traces in the recycle bin.

4. Implementation responsibility

4.1. All staff members are responsible for the implementation of the policy; however, the Principal and the Registrar are mainly responsible for the observation and implementation of the policy.

5. Monitoring

5.1. The implementation of the Act is monitored through random checks and through scheduled data collection and management checks.

6. Policy Review

6.1. This policy will be reviewed on a regular basis in accordance with legislative developments and the need for good practice, using the Information Commissioner's Office guidelines.

6.2. The Registrar will be the responsible person to make sure that the policy is reviewed at least once in a year and circulated as per requirements.