DATA PROTECTION POLICY

TSMR Data Protection Policy

1. Purpose

The purpose of this policy is to ensure that the company complies fully with its legal obligations in relation to the protection of personal data that it holds about or concerning any individual. All employees and officers of the company must familiarise themselves fully with its contents and ensure that its terms are applied fully in relation to the handling or "processing" of personal data.

Those employees whose job involves the handling of personal data will receive appropriate training at their induction[1] and, as required during their employment, and the procedures for obtaining, retaining, updating, using, transporting, sending and destroying personal data. All of these functions are strictly confidential and any employee handling personal data in breach of the Institute's data protection policy may face disciplinary charges that may, in serious cases, result in dismissal.

This policy concerns personal data held by the Institute in relation to any person, whether they are, were or are about to become employees of the Institute or any customer, supplier or contact. Personal data is described below in more detail, but the concept is very broad and may include any information about any individual, held by the Institute.

Data protection laws are overseen by the Information Commissioner who has powers to take legal action against businesses or individuals acting unlawfully. Any employee may make themselves individually liable to legal action by the Information Commissioner and/or by any individual whose information they have disclosed in breach of data protection legislation and who suffers loss as a result. There have also been very high profile cases involving loss of data in breach of the legislation giving rise to very real damage to the reputation of the organisations concerned. This policy is designed to prevent such potential damage to the company and its employees and to ensure that personal data processed by the company is dealt with in full compliance with the law.

---

[1] Training should be provided for any staff who are involved in the handling of personal data.

2. Definition and scope

The law contains some important concepts that define the obligations of the Institute and its employees. Although most employees are not expected to remember detailed legal definitions, a general understanding of the concepts is required to avoid inadvertent breaches and to ensure that employees can take further advice in relation to any particular situation that may give rise to concern. The company will nominate an individual responsible for data processing and compliance with data protection legislation. Any questions or concerns relating to the Institute's or any individual employee's responsibilities should be referred to the employee's line manager.

Some important terms used in the data protection legislation have been broadly defined below to assist employees to carry out their duties for the Institute properly and lawfully. They are close to but are not strictly legal definitions. Applying them, however, will greatly assist in legal compliance as they are designed to avoid complex legal points, and are, therefore, broadly defined.

The Policy

The Principles require that personal information

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,

2. Shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes,

3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed,

4. Shall be accurate and, where necessary, kept up to date,

5. Shall not be kept for longer than is necessary for that purpose or those purposes,

6. Shall be processed in accordance with the rights of data subjects under the Act,

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data,

8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Institute will, through appropriate management, strict application of criteria and controls:

1. Observe fully conditions regarding the fair collection and use of information,

2. Meet its legal obligations to specify the purposes, for which information is used,

3. Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements,

4. Ensure the quality of information used,

5. Apply strict checks to determine the length of time information is held,

6. Ensure that the rights of people about whom information is held, can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information)
7. Take appropriate technical and organisational security measures to safeguard personal information,

8. Ensure that personal information is not transferred abroad without suitable safeguards,

9. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,

10. Set out clear procedures for responding to requests for information.

In addition, the Institute will ensure that:

1. There is someone with specific responsibility for Data Protection. The school's Data Protection Officer; attention Theo. (tgokah@tsmr.uk)

2. Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice

3. Everyone managing and handling personal information is appropriately trained to do so,

4. Everyone managing and handling personal information is appropriately supervised

5. Anybody wanting to make enquiries about handling personal information knows what to do

6. Queries about handling personal information are promptly and courteously dealt with

7. Methods of handling personal information are clearly described

8. A regular review and audit is made of the way personal information is held, managed and used,

9. Methods of handling personal information are regularly assessed and evaluated

10. Performance with handling personal information is regularly assessed and evaluated

11. A breach of the rules and procedures identified in this policy by a member of staff may lead to disciplinary action being taken

12. A breach of the rules and procedures identified in this policy by a Member is a potential breach of the Code of Conduct.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

Cardiff, 2018