General Data Protection Regulation (2018)

Data Protection Principles

OE and all employees must comply with the principles found in the GDPR (2018) at all times in their information-handling practices.

To summarise, the principles say that personal data must be:

1. Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that the employee has given their consent to the processing, or the processing is necessary for the various purposes set out in the Act.
Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:
• Race or ethnic origin.
• Political opinions and trade union membership.
• Religious or other beliefs.
• Physical or mental health or condition.
• Sexual life.
• Criminal offences, both committed and alleged.

2. Obtained only for one or more specified and lawful purposes, and must not be processed in any manner incompatible with those purposes.

3. Adequate, relevant and not excessive in relation to the purposes for which it is processed. OE will review employees' personnel files on a regular basis to ensure they do not contain a backlog of out of date or irrelevant information and to check there is a sound business reason requiring information to continue to be held.

4. Accurate and, where necessary, kept up-to-date. If your personal information changes, for example you change address or you get married and change your surname, you must inform your line manager as soon as practicable so that the Company's records can be updated. The Company cannot be responsible for any such errors unless the employee has notified the Company of the relevant change.

5. Not kept for longer than is necessary. The Company will keep personnel files for no longer than two years after an employee has left the Company's employment. Different categories of data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a particular period of time will be destroyed after approximately one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.

6. Processed in accordance with the rights of employees under the Act.

7. Secure. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data. Personnel files are confidential and are stored as such. Only authorised employees have access to these files. Files will not be removed from their normal place of storage without good reason. Data held on computer is also stored confidentially by means of password and again only authorised employees have access to that data. The Company has network back-up procedures to ensure that data on computer cannot be accidentally lost or destroyed.

8. Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection relation to the processing of personal data.

Employee Consent to Data Being Held

OE holds personal data about its employees and, by signing your contract of employment, you have consented to that data about you being processed by the Company. Agreement to the Company processing your personal data is a condition of your employment. The Company also holds limited sensitive personal data about its employees and, by signing this policy, you give your explicit consent to our holding and processing that data, for example sickness absence records, particular health needs and equal opportunities monitoring data.

Employees' obligations in relation to personal information

You should ensure you comply with the following guidelines at all times:

· Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone, either accidentally or otherwise, from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this.
· Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.
· Only transmit personal information between locations by fax or email if a secure network is in place, for example, encryption is used for email.
· If you receive a request for personal information about another employee, you should forward this to the Director, who will be responsible for dealing with such requests.
· Ensure that any personal data which you hold is kept securely, either in a locked place, if it is computerised, it is password protected.
Compliance with the Act is the responsibility of all employees.

Employees are also reminded to ensure files containing sensitive information are not left on desks when unattended and are stored properly and securely. When sending student information via email

employees are reminded that this information should be held in a password protected file, to ensure its security.

Any online email and accounts held for the company should be password protected, and where possible, two-step verification should be in use to ensure security.

Any questions or concerns about the interpretation of this policy should be taken up with the Managing Director.