- Present their licence, and any other documents required, for inspection on request (normally annually).
- Co-operate with monitoring, reporting and investigation procedures.

12. Data protection policy

During your work you may come into contact with or use confidential information about employees, clients and customers, for example their names and home addresses. The **Data Protection Act 2018** contains principles affecting employees' and other personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system. The purpose of these rules is to ensure you do not breach the Act. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from Mr Ng, the Employer's Data Protection Officer. You should be aware that you can be criminally liable if you knowingly or recklessly disclose personal data in breach of the Act. A serious breach of data protection is also a disciplinary offence and will be dealt with under the Employer's disciplinary procedures. If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

The data protection principles

There are eight data protection principles that are central to the Act. The Employer and all its employees must always comply with these principles in its information-handling practices. In brief, 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 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 not processed in a manner incompatible with those purposes.

3. Adequate, relevant and not excessive. The Employer will review personnel files on an annual basis to ensure they do not contain a backlog of out-of-date information and to check there is a sound business reason requiring information to continue to be held.

4. Accurate and kept up to date. If your personal information changes, for example you change address, you must inform the Office Manager as soon as practicable so that the Employer's records can be updated. The Employer cannot be held responsible for any errors unless you have notified the Employer

of the relevant change.

5. Not kept for longer than is necessary. The Employer will keep personnel files for no longer than six years after termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which the Employer decides it does not need to hold for a period will be destroyed after 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, technical and organisational measures will 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 in locked filing cabinets. Only authorised staff have access to these files. Files will not be removed from their normal place of storage without good reason. Data stored on diskettes or other removable media will be kept in locked filing cabinets. Data held on computer will be stored confidentially by means of password protection, encryption or coding and again only authorised employees have access to that data. The Employer has network backup 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 ensures an adequate level of protection for the processing of personal data.

Your consent to personal information being held

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

Your right to access personal information

You have the right, on request, to receive a copy of the personal information that the Employer holds about you, including your personnel file, and to demand that any inaccurate data be corrected or removed. You have the right on request:

- to be told by the Employer whether and for what purpose personal data about you is being processed
- to be given a description of the data and the recipients to whom it may be disclosed
- to have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data
- to be informed of the logic involved in computerised decision-making.

Upon request, the Employer will provide you with a statement regarding the personal data held about you. This will state all the types of personal data the Employer holds and processes about you and the reasons for which they are processed. If you wish to access a copy of any personal data being held about you, you must make a written request for this and the Employer reserves the right to charge you a fee of up to £10. To make a request, please complete a Personal Data Subject Access Request Form, which can be obtained from the Data Protection Officer.

If you wish to make a complaint that these rules are not being followed in respect of personal data the

Employer holds about you, you should raise the matter with the Data Protection Officer. If the matter is not resolved to your satisfaction, it should be raised as a formal grievance under the Employer's grievance procedure.

Your obligations in relation to personal information

You should ensure you always comply with the following guidelines :

- do not give out confidential personal information except to the data subject. It should not be given to someone 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 e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail
- if you receive a request for personal information about another employee, you should forward this to the Office Manager who will be responsible for dealing with such requests
- ensure any personal data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is password protected
- compliance with the Act is your responsibility. If you have any questions or concerns about the interpretation of these rules, take this up with the Data Protection Officer.