20. COMPUTERS, E-MAILS AND INTERNET USE

- The Employer operates virus protection software. No software or program or similar may be loaded on the Employer's computer system unless and until it has been checked for viruses.
- You are not permitted to copy the Employer's software, other than when this is necessary in the normal course of your duties.
- On leaving the Employer's employment, and at any other time at the Employer's request, you are required to hand back any of the Employer's information and data held by you in computer-useable format.
- You are required to take any necessary security measures to prevent unauthorised access to, alteration, disclosure and destruction of personal data, and accidental loss and destruction of Employer data.
- You must not access, process, use, or disclose any data or password other than is necessary for the proper performance of your duties.
- Use of internet must be for business purposes only in the course of carrying out your duties. Occasional use of the internet for personal use is permitted at break and lunch times but is subject to compliance with rules laid down by The Association. Unauthorised use of the internet will constitute misconduct.
- You must not download software from the internet onto the Employer's system without prior permission.
- You are not permitted to download any video-based material or content that requires a TV licence.
- You are not permitted to divert any work e-mails to your personal device without prior consent of your Line Manager.

Misuse of the e-mail system by transmission of any material, which is defamatory, offensive or obscene, untrue or malicious, or in breach of copyright will constitute gross misconduct. In particular, the processing (which means storing, sending or downloading) of sexually explicit material will constitute gross misconduct. You must not use your Association's e-mail address for your own personal correspondence.

21. SOCIAL NETWORKING POLICY

A social network service focuses on the building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others.

Most social network services are primarily web based and provide a collection of various ways for users to interact, such as chat, messaging, email, video, voice chat, file sharing, blogging, discussion groups. Social networks include, but not limited to Facebook, Twitter, LinkedIn, Instagram, Whatsapp, Snapchat, Messenger and personal blogs.

The purpose of a social networking policy

- To help the Association against potential liability;
- To give employees clear guidance on what can and can't occur in relation to the Association or other employees;
- To help employees separate their professional and personal communication;
- To comply with the law on data protection, discrimination and protecting employees.

Standards employees are required to comply with are as follows:

- Employees will not maintain any site that contains personal identifiable information of the Association or clients.
- Employees will not maintain a site that contains photographs of clients.
- Employees will not maintain a site that contains identifiable information of a client or an employee in relation to their performance and character.
- Employees will not maintain a site that contains photographs of another employee taken in the work situation or in their working uniform.
- Employees will not maintain a site that contains defamatory statements about the Association, its current or ex-employee, the Association's services or contractors.
- Employees must not express opinions on the sites that purport to represent their own views on the Association.
- Employees must never post a comment on the sites that purports to represent the views of the Association without first consulting their Line Manager.
- Employees must not breach the Association's confidential information.

As an employee of the Association, the Association has a reasonable and lawful expectation that staff will not bring the organisation into disrepute, this is extended to the home environment as well. Any grievance with the organisation should be processed through procedures and policies already in place and dealt with within the work environment.

If employees become aware of a breach in this policy, they should contact their line manager in the first instance if it is appropriate to do so. It is possible such a matter may be resolved locally. If this is not the case and if staff, are found to have contravened this policy, disciplinary sanctions, up to and including dismissal can occur.

The Association reserves the right to access and monitor all emails and internet activities carried out on Association equipment including the use of any social networking site.