Public Interest Disclosure Policy

(Whistleblowing Policy)

The Public Interest Disclosure Act 1999 gives legal protection to employees against victimisation for publicly disclosing legitimate concerns. This policy is designed to enable employees to raise concerns internally about malpractice or wrongdoing within the organisation, without fear of reprisals.

Employees should raise concerns if they suspect:

- financial impropriety or fraud
- failure to comply with legal obligations
- criminal activity
- dangers to health & safety
- improper conduct or unethical behaviour
- actions contrary to Company policies, procedures or instructions

This policy and procedure are not intended to be a mechanism for staff to challenge decisions with which they disagree or to settle personal scores, but is reserved for raising serious concerns about malpractice.

The Public Interest Disclosure Act sets the following rules:

- The disclosure must be made in the public interest
- There must be a reasonable belief that it is substantially true
- Employees must not act maliciously or make false allegations
- Employees must not seek any personal gain

No action will be taken against individuals making allegations in good faith which are found to be untrue after investigation. If, however, the allegations are judged to be malicious, disciplinary action may be taken against the individual.

Procedure for making a protected disclosure

Concerns should initially be reported to an appropriate manager or director. If necessary, employees may be supported by a fellow worker or trade union representative.

The complaint will be investigated as speedily as possible and the individual informed of what action, if any, is to be taken.

Confidentiality

Employees making a protected disclosure in good faith will not suffer any detriment and all disclosures will be treated in a confidential manner. Employees are encouraged to make signed statements of any disclosures they may make, but the identity of the individual will normally be kept confidential unless he or she agrees otherwise.

However, for example in the case of criminal activity where the police may become involved, it may not be possible to guarantee anonymity.

Data Protection Policy
In the course of your work you may come into contact with or use confidential information about other employees or business associates, for example their home addresses. The General Data Protection Act 2018 (GDPR) 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 that you do not breach the Act.

You should be aware that, under the Act, you are personally accountable for your actions and can be held criminally liable if you knowingly, or recklessly, breach it. Any serious breach of data protection will also be regarded as misconduct and will be dealt with under the Company'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. In brief, the principles say that personal data must be:

- 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.

- Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.

- Adequate, relevant and not excessive. The Company 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.

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

- Not kept for longer than is necessary. The Company 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 Company decides it does not need to hold for a period of time will be destroyed after one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.

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

- Safeguarded by appropriate measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personnel files are confidential and are stored in locked filing cabinets. Data held on computer will be stored confidentially by means of password protection, encryption or coding. The Company has network backup procedures to ensure that data on computer cannot be accidentally lost or destroyed.

- 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 Company holds personal data about you. By signing your contract of employment, you have consented to that data 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 your contract of employment, you give your explicit consent to the Company holding and processing that data, for example sickness absence records and health needs.

Your obligations in relation to the personal information of others
You should ensure you comply with the following guidelines at all times:

- do not give out confidential personal information without the prior consent of a director. In particular, personal information should not be given to anyone 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 you should forward this to a director.
- 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 about the interpretation of these rules, please contact a director.