Monitoring policy

Policy statement

The Company carries out workplace monitoring for a variety of reasons. Because monitoring includes the processing of employee data, its operation is captured by the provisions of the General Data Protection Regulation and the current Data Protection Act.

The lawful basis which applies to the Company's monitoring processes is legal obligation and legitimate interests.

The information and data gathered through monitoring will only be used for the purpose it was carried out for, unless the Company identifies issues such as a breach of health and safety.

The person with overall responsibility for the operation of this policy is the CFO. Only the CFO, CEO or Group HR Business Partner may authorise any monitoring of employees.

As monitoring may intrude on Company employees' private lives, monitoring will be carried out only in accordance with the General Data Protection Regulation and the current Data Protection Act. The Company will uphold a degree of privacy at work and where monitoring is required or necessary, employees will be made aware of the extent of any monitoring together with the reasons as to why.

The Group HR Business Partner will ensure the Company is aware of its responsibilities under the General Data Protection Regulation and the current Data Protection Act. Access to the information and data collected will be secure and restricted to authorised employees.

Summary of types of monitoring

This policy supplements the Company's policies on communications and provides for monitoring of the following types:

- Crime and fraud prevention and detection
- CCTV scheme and security systems
- Company telephone infrastructure
- Computer systems
- Bag searches
- Internet and email usage
- Data protection

Monitoring of the above systems is carried out to fulfil the Company's legal obligations as an employer as well as to secure their effective operation and for business reasons. Monitoring is carried out to the extent permitted or required by applicable law and as necessary and justifiable for business purposes.

Computer, internet and email monitoring

The Company may randomly check emails or use software to check if employees are sending, or receiving, inappropriate emails.

This monitoring may be necessary to investigate alleged misconduct, detect or prevent crime, deal with any issues surrounding the Company's reputation, or retrieve content if an employee is absent. Performance of the system or the employee may be assessed through email and internet monitoring. Monitoring may be required to comply with legal obligations or detect/prevent crime.

Personal usage may have been permitted by a line manager or other senior colleague and monitoring will include every effort to ensure personal emails are not accessed where personal use can be clearly

distinguished from business use.

CCTV monitoring

The Company routinely operates a CCTV scheme to check that health and safety rules are being complied with or to assist in the prevention of crime, for instance theft.

The CCTV scheme records data in all TechPoint locations.

The CCTV scheme is run in compliance with the current Data Protection Act and the recordings may be used to assist in investigations for internal disciplinary and grievance purposes where there are justified business reasons for the viewing of such recordings.

Phone monitoring

The Company keeps recordings of telephone calls that come into the business for training purposes, for dealing with complaints from customers and to comply with legal obligations. The Company checks telephone logs to detect misuse of telecommunications.

Phone monitoring is used to assess performance, ensure compliance with Company telephony policies and protect the Company's reputation. Phone monitoring assists with investigations into alleged misconduct.

Monitoring extends to fixed line phones and mobile telephones.

Personal usage may have been permitted by a line manager or other senior colleague and monitoring will include every effort to ensure personal calls are not accessed where personal use can be clearly distinguished from business use.

Misconduct

Employee monitoring data may be used for disciplinary proceedings against employees.

Employees will be provided with the relevant data from the monitoring systems/processes in advance of the meeting.

Covert monitoring

Covert monitoring is only deployed where the Company believes employee(s) are carrying out a crime or other criminal activity. Covert monitoring may take place to investigate such suspicion where the Company intends to involve the police.

Additional monitoring

The Company may, if appropriate, consult with employees in advance if it requires any additional monitoring not covered by this policy. The purpose of the additional monitoring will be identified, together with the type of monitoring necessary and any limits to achieve that purpose. There may be impacts on affected employees that the Company will consider prior to introducing any additional monitoring. Notice will be provided to employees setting out why the Company is introducing additional monitoring and the standards under which employees should operate.

Retention of monitoring data

All data captured as a result of employee monitoring will be kept securely.