EMPLOYEE MONITORING POLICY
OCTOBER 2023

CONTENTS PAGE

1. INTRODUCTION & DEFINITION

1.1 The Company, like many large organisations, carries out employee monitoring in order to safeguard employees, to protect its business interests and to protect the interests of its customers. Employee monitoring is governed by:

- the Data Protection Act 2018, the UK General Data Protection Regulation 2018 (UK GDPR) and the accompanying good practice principles set out in the Information Commissioner's Employment Practices Code and the supplementary Guidance issued by the Commissioner to support the Code;
- Article 8 of the European Convention on Human Rights (right to respect for private and family life, and for correspondence); and
- the Regulations of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations made under the Act.

1.2 The Data Protection Employment Practices Code defines monitoring as those activities that are taking place, or are planned to take place, which set out to collect information about workers by keeping them under some form of observation, normally with a view to checking their performance or conduct. This can be done directly, perhaps by examining employee work output, or indirectly, such as the automated electronic monitoring of the use of IT systems.

1.3 The purpose of this policy is to set out the details of how and for what purpose the Company monitors its employees, in accordance with the legislation detailed in 1.1 above. Examples of employee monitoring within the Company include:

- Company internet and e-mail usage;
- Surveillance technology (CCTV, dash cams, body cams and drones);
- Company telephones and mobiles; and
- Vehicle telematics.

1.4 The Company carries out both systemic and occasional monitoring:

- '**Systematic**' monitoring is where an employer monitors all workers, or particular groups of workers, as a matter of routine, e.g. the installation of telematics devices in company vehicles.

- '**Occasional**' monitoring is where an employer introduces monitoring as a short-term measure in response to a particular problem or need, e.g. the use of CCTV surveillance in an investigation into an allegation of theft of company property.

1.5 The Company may (under circumstances defined below) exercise its right to intercept any communication to and/or from employees, workers, agents or customers using its telephony or data networks.

1.6 The use of employee monitoring within the Company is to promote and ensure:

- compliance with its health, safety and welfare obligations;
- the protection of its business interests;
- the protection of its customers' interests;
- its systems and assets are not being misused (including excessive use); and
- its assets and infrastructure are used effectively and appropriately for business purposes.

1.7 Employee monitoring shall not be used for:
- any unauthorised purposes, being any purpose not set out at 1.6 above; or
- any personal interests, e.g. to check the whereabouts of an individual for personal, non-business reasons or simply out of curiosity.

1.8 The Company shall ensure that personal data derived from its employee monitoring activities (and that of third-party suppliers/data processors) is treated lawfully and correctly, including accuracy, and is not excessive in relation to the purpose for which it is kept. All data shall be processed in accordance with the rights of data subjects and be compliant with the GDPR. Where required, Data Protection Impact Assessments (DPIAs) and Legitimate Interest Assessments (LIAs) will be completed.

1.9 Privacy

1.9.1 The Company takes the privacy of its employees very seriously. To assess and establish compliance with the GDPR (and other applicable regulations), including fair, lawful and transparent processing, processing only for specified, explicit and legitimate purposes, adequate, necessary and limited processing, appropriate retention and appropriate security (both technical and organisational) governing the processing, the Company shall carry out Data Protection Impact Assessments (DPIA) and Legitimate Interest Assessments (LIA), where appropriate, regarding the monitoring activities to ensure a balance between employee privacy and the legitimate interests of the business.

1.10 Other policies/procedures relating to this document include:
- Acceptable Use of IT Policy
- Social Media Policy
- CCTV Policy
- Telematics Policy
- Drugs & Alcohol Policy
- Supporting Attendance Policy
- Disciplinary Policy
- Grievance Policy
- Data Subject Access Requests

2. SCOPE

2.1 This is a group level policy that applies to all employees of Anglian Water Group Limited and its subsidiary companies, with the exception of Anglian Water (Ireland) Limited and Wave Limited (and their respective subsidiaries, which include Celtic Anglian Water and Anglian Water Business (National)).

3. STATUS

3.1 This policy is subject to regular review by the Company and is updated as appropriate.

4. POLICY OWNER

4.1 Head of Employee Relations.

5. INTERNET/E-MAIL

5.1 Company internet and e-mail usage (content, volume and engagement levels) is monitored by automated software, which is available 24 hours a day, seven days per week.

5.2 Whilst the e-mail data is not monitored closely at all times, information can be accessed covering any period of the day, either in or outside the normal working hours of an employee.

5.3. Access to inappropriate and unlawful sites is restricted, e.g. websites of a sexual nature and online gambling and gaming.

5.4 The Company's Acceptable Use of IT Policy details what internet / e-mail activity is permitted and prohibited.

5.5 Where high usage volumes or inappropriate content is identified, manual audits/investigations shall take place. The results of these investigations may be referred for disciplinary action (see the Company's Disciplinary Policy & Procedure).

5.6 Requests for **specific occasional monitoring** of accounts and systems (including surveillance activities such as CCTV, dash cams and body cams) can be made, where there are reasonable grounds for these requests, e.g.

- evidence to suggest involvement in criminal activity;
- evidence to suggest inappropriate access to/downloading of commercially sensitive information;
- a report of an employee accessing of inappropriate sites containing, racist, sexist, obscene or pornographic content;
- suspected cyber bullying and/or harassment;
- a report suggesting excessive use of IT or other business systems;
- evidence to suggest the downloading of non-business or non-essential material; and
- a report of a suspected serious breach of Company policy, e.g. personal use of a company commercial vehicle.

5.7 Requests for specific occasional monitoring must be made in writing and addressed to the Group People Director, HR Operations Director, Head of Employee Relations or nominated person with delegated authority for approval.

5.8 Where inappropriate use of IT Systems is suspected and there is a high level of risk/impact to the Company's operations as assessed and determined by the Group People Director, HR Operations Director, Head of Employee Relations or nominated person with delegated authority, IT accounts/access may be frozen or locked.

5.9 The Company uses an email filtering system to screen incoming and outgoing mail (including attachments) and to protect the Company's systems from:

- virus attack;
- spam and phishing;
- denial of service attack;
- email content deemed contrary to Company policies regarding acceptable mail;

- prohibited file attachments such as MP3/video files that could be subject to copyright protection.

Where this filtering system stops legitimate business mail by placing the message in quarantine the message can be released by the User.

5.10 Email may be quarantined and/or deleted without the sender or intended recipient being notified.

5.11 The Company reserves the right to monitor email and messaging accounts / gain access to email or messaging accounts in order to conduct internal investigations into allegations of potential breaches of the Company's Codes of Conduct or Policies and Guidance.

5.12 In order to gain access to an individual's email accounts, the appointed Investigating Manager must submit a request to Group People Director, HR Operations Director, Head of Employee Relations or nominated person with delegated authority*, explaining why the access is required, and the steps that will be taken to minimise the risk of unnecessary intrusion.

*These are the only people with authority to grant access to an individual's email accounts.

6. SURVEILLANCE TECHNOLOGY

6.1 Surveillance technology, such as CCTV, dash cams, body cams and drones, is used primarily for security purposes, e.g. on sites to monitor entrances, car parks and work areas. The use and storage of this footage shall comply with data protection guidelines. See the Company's Policy and Code of Practice for the use of Surveillance Equipment.

6.2 In exceptional circumstances, e.g. suspected gross misconduct, the Company reserves the right to operate covert surveillance.

7. COMPANY TELEPHONE & MOBILES

7.1 Company telephone calls may be recorded for training and monitoring purposes, e.g. in Customer Contact Centre and Operational Management Centre (OMC). Employees and customers shall be advised by the privacy notice, by recorded messages, by the training provided to employees, or directly from the agent handling the call when calls are to be recorded and monitored.

7.2 Requests for access to a specific telephone call recording can be made:
- in order to check or verify information for a customer;
- to respond to a customer complaint;
- where there are reasonable grounds to suspect:
  - employee involvement in criminal activity; or
  - serious breach of Company policy by an employee.

7.3 Requests for planned, specific monitoring of telephone/mobile accounts can be made, where there are reasonable grounds for these requests, e.g. suspected:
- evidence to suggest involvement in criminal activity;
- a report of an employee accessing of inappropriate sites containing, racist, sexist, obscene or pornographic content;

- suspected cyber bullying and/or harassment;
- a report suggesting excessive personal use of IT or other business systems;
- evidence to suggest the downloading of non-business or non-essential material; and
- a report of a suspected serious breach of Company policy, e.g. breach of the Dignity at Work policy.

7.4 Requests for specific occasional monitoring must be made in writing and addressed to the Group People Director, HR Operations Director, Head of Employee Relations or nominated person with delegated authority for approval.

8. TELEMATICS

8.1 Telematics information within the Company is used primarily as a Health & Safety tool to encourage safer driving behaviours, reduce accidents and as a tool to aid the efficient scheduling of operational jobs.

8.2 Users of the Telematics devices are made aware in the Telematics Policy that all activity, system access and use is centrally monitored and reported.

8.3 All telematics monitoring in Company vehicles shall be processed in accordance with the Telematics PIA and Telematics Policy.

9. OTHER MONITORING ACTIVITY

9.1 Driver Licences

9.1.1 All external candidates, or internal candidates moving to a post where they qualify for an annual electronic driving licence check, are expected to complete a driving licence mandate form. Details provided will be validated electronically by a third party in order to demonstrate that the candidate is entitled to drive in the UK and to drive the required category of vehicle. Regular checks will be made of driver licences and in particular if an individual receives a Notice of Intended Prosecution from the Police for a driving related offence. All checks shall be processed in accordance with the Driver Licence PIA.

9.2 Drugs and Alcohol

9.2.1 The Company's Drugs & Alcohol Policy provides for the testing of employees at recruitment and during their employment by way of 'for cause' or 'random' testing with the support of a specialist third party provider. All drugs and alcohol tests shall be processed in accordance with the Drugs and Alcohol PIA and Drug & Alcohol Policy.

9.3 Sick Absence

9.3.1 The Company records and monitors individual sickness absence with the support of a specialist third party provider. Sickness absence records shall be maintained and monitored in accordance with the sickness absence PIA and Supporting Attendance Policy & Procedure.

9.4 Medical Records/Reports

9.4.1 Individual medical records/reports shall be maintained and processed in accordance with the GDPR Act, May 2018. Access to these records shall be managed in accordance with the Access to Medical Records Act 1988 and Access to Medical Reports Act 1990 and is detailed in the Management of Medical Records Disclosure Procedure.

9.5 Workday

9.5.1 Workday is the integrated HR/Payroll system that holds all employee data, from recruitment to leaving employment. In addition to the personal data held on this system, Workday is used to hold and monitor information about employee's training and performance records. All information is held and processed in accordance with the GDPR Act, May 2018.

9.6 Personnel Security Risk Register

9.6.1 The Company maintains a register of positions that require higher level security clearance in order to reduce the risk of insider activity and protect the Company's assets. Employees who hold these positions are subject to regular security checks, the outcome of which are recorded on the Risk Register. All information is held and processed in accordance with the GDPR Act, May 2018.

9.7 General

9.7.1 The Company reserves the right to monitor other areas for business purposes as detailed in the following non-exhaustive list of examples:

- time recording, e.g. logging in out and of sites using an ID card, the signing in/out book or the local control system in place and the use of PMS (work planning / health & safety); and
- retention of vehicle registration data (site security and parking).

9.7.2 The Company reserves the right, in exceptional circumstances, to undertake specific monitoring, which is proportionate and based on legitimate need.

10. DATA SUBJECT ACCESS REQUESTS

10.1 An employee, or any individual, may submit a Data Subject Access Request (DSAR) to obtain access to and information about the data containing their personal information generated by the Company's monitoring activities.

10.2 Employees have a number of other rights in respect of personal data under the GDPR and Data Protection Act 2018, e.g. the right to be informed, the right of access, the right to object, the right to erasure and the right of rectification.

10.3 Guidance on DSARs and the procedure to follow can be found on Lighthouse or by following this link.

10.4 Any request to exercise individual's GDPR and Data Protection rights can be made electronically, via letter or verbally to line managers or via the DSAR inbox.

11. COMPLAINTS PROCEDURE

11.1 Any individual who believes that any monitoring activity or system is being undertaken or used unlawfully or inappropriately or has any concern regarding monitoring activities can raise a complaint via their line manager, or more formally through the Company's Grievance Procedure or Whistleblowing Procedure.

11.2 In addition to the internal grievance procedure, individual employees have the right to raise any data protection complaint to the Information Commissioner's Office by visiting their website.

12. FURTHER ASSISTANCE

Please contact your Line Manager or Employee Relations Manager/Advisor for further assistance.

LAST REVIEWED
October 2023