HINCKLEY AND BOSWORTH BOROUGH COUNCIL

WORKPLACE SURVEILLANCE POLICY

1. Introduction

1.1 The council recognises its obligations to ensure where reasonable practicable, a safe and healthy workplace. Employers may monitor, using certain surveillance devices, to safeguard against any risks associated with employees, customers and others in the workplace and assist management to optimise performance, improve efficiency and customer service.

1.2 Whilst the council does not intend to use surveillance methods or monitor staff movements, it may from time to time, or with cause, access surveillance systems and data records in order to investigate complaints or conduct matters. This data may be used as evidence in work place investigations as appropriate.

1.3 Surveillance data will be submitted to the police, upon request, for the purpose of the prevention and detection of crime.

2. Purpose

2.1 This policy will set out how the council will monitor the use of its information and communication technology systems, along with the use of surveillance cameras (CCTV, in-vehicle cameras and body worn cameras).

3. Scope

3.1 This policy applies to all council employees including agency staff, consultants and contractors (workers).

4. Communication of this policy

4.1 It is management's responsibility to make users aware of this policy by:

- Introducing this policy as part of the induction process
- Informing staff that they are accepting terms of the council's Acceptable Usage Policy for Email, the Internet and Corporate Network Access
- Regular staff training in regard to the principals of the Data Protection Act 1998 (General Data Protection Regulation from 25 May 2018)

5. Privacy

5.1 This policy seeks to strike the balance between respecting staff privacy whilst allowing the necessary monitoring required meeting the council's business and legal obligations. Staff will be informed, through this policy, that monitoring is taking place, what form this will take and the reasons for monitoring.

5.2 The council recognises that employees have a legitimate expectation that they should be able to keep their private lives private and they are entitled to a degree of privacy in the work place. Therefore this policy will always be used in a way that is consistent and compliant with the Data Protection Act 1998

(General Data Protection Regulation from 25 May 2018) and the Human Rights Act 1998.

6. Types of surveillance equipment in use

6.1 The types of workplace surveillance that the council will use include the following:

- **Camera surveillance**
    - CCTV based at council properties (including parks and car parks) and with commercial estates - please refer to the CCTV procedure
    - Vehicle cameras (refuse trucks only) - please refer to the guidance on surveillance captured in council vehicles
    - Body-Worn Video – please refer to the Body-Worn Video Standard Operating Procedure
- **Computer surveillance**

  This includes electronic communications such as internet usage, software access and email use - please refer to the council's Acceptable Usage Policy for Email, the Internet and Corporate Network Access
- **Tracking surveillance**
    - Council-owned vehicles with tracking devices - please refer to Acceptable Use of Vehicles and Equipment Policy
    - Door Access system for council buildings
- **Mobile telephone data**

  Telephone usage activity on work mobiles - please refer to Corporate Mobile Device Policy

Data and information is monitored and gathered by the council in the interest of safety and security. It may also include information about employees' activities to ensure that they carry out their duties efficiently and safely, for training purposes and record keeping.

7. How the surveillance is carried out

7.1 **Camera surveillance**

CCTV - The council uses camera surveillance to monitor security and to provide employee and public safety. Areas that are subject to camera surveillance will display appropriate signage to inform employees and the public in accordance with the Data Protection Act 1998 (General Data Protection Regulation from 25 May 2018). Data is stored for 30 days.

Vehicle Cameras – cameras are installed on council vehicles (HGV) primarily for the prevention and detection of crime. It can also be used as evidence in

accidents and potential claims against the vehicles by residents. Data is stored for 30 days.

Body-Worn Video – used by officers undertaking front-line enforcement duties such as investigating suspected criminal acts who are vulnerable to abuse and threatening behaviour, both verbal and physical, from members of the public. Data is stored for 6 months (unless action is being taken).

7.2 Computer surveillance

Computer surveillance is used for the general security of the council's property and assets, for the protection of council related information and to ensure that the council's computer and mobile resources are not misused. Access to and usage of services include: Email use, internet access and network access which may be monitored (including details of websites visited) for performance and management purposes.

The council uses software applications to record activity such as: logon details and times, email activity, and internet access. Email traffic is not routinely read however it is continually monitored by software to ensure the security and stability of the council's network. The council reserves the right to access any files sent or received over the network to ensure compliance with IT policies. Internet usage is monitored by a web security filter to restrict access to inappropriate sites.

7.3 Tracking surveillance

Vehicles Surveillance - GPS devices have been fitted to council vehicles to assist in council operations, provide security of the vehicle and to assist in the safety of staff. As part of the council's fleet management procedures the council is required to audit vehicle movements including:

- Locations visited
- Time spent at locations
- Days and times of journeys
- Speed of journeys

The council also has a legal obligation to track vehicles when tachographs are fitted i.e. Lorries and vehicles over 5.5 tonnes. Data is stored for 12 months.

Building surveillance – for security purposes the council undertakes surveillance of workers through the operation of building access swipe cards (TDSI Door Access system). Data is stored for 90 days.

8. When data is accessed

8.1 Continuity of service

The council has the right to inspect the data on its ICT systems to fulfil business need; this includes access when a user is unexpectedly absent or is on annual leave. The staff member will be notified, where practicable, before any access is made.

8.2 **Complaints, accidents and monitoring**

Vehicle surveillance access - footage is only downloaded in the following circumstances:

- When a complaint about staff conduct has been received from a member of the public
- Following an accident / incident (alleged or otherwise) either involving the vehicle or a member of staff in the vicinity of the vehicle
- For monitoring and auditing of health and safety practices

In these circumstances, footage may only be viewed with the consent of Head of Street Scene Services, the Business Development and Street Scene Manager or Director (Environment and Planning).

Any requests to view footage for any other reason may only be viewed with the consent of either Director (Corporate Services), the Information Governance Officer or the HR and Transformation Manager.

Footage recorded from refuse wagons is only available to view for 30 days unless downloaded. A log book will be kept to record requests, action taken and the outcome.

Camera surveillance access (CCTV) – the council's system has a recording facility and a live on-premises capability but no off-site live viewing facility.

Footage is only viewed in the following circumstances:

- For the prevention and detection of crime
- To provide evidence in civil proceedings or tribunals
- For monitoring and auditing of health and safety practices

Access may only be given to designated council staff to view data following approval of the Director (Corporate Services) or the Information Governance Officer.

In respect of commercial premises, permission may also be given by the Commercial Estates Surveyor, Principal Surveyor or Senior Surveyor.

A log book will be kept to record requests, action taken and the outcome.

Body-Worn Video access - Viewing of recorded images should take place in a restricted area and access may only be given to designated council staff to view data following approval of the Director (Corporate Services) or the Information Governance Officer. Unauthorised persons shall not be allowed access to that area when a viewing is taking place and arrangements should be put in place to ensure that viewing screens cannot be overlooked.

8.3 **Investigation – Disciplinary matters**

Managers, who strongly suspect employees of misconduct and believe that the data from any of the above sources may support their case, should primarily discuss their concerns with the HR and Transformation Manager (who will follow the relevant procedures for those documents to be requested and examined).

To seek camera footage, the HR and Transformation Manager will follow the procedures outlined within 8.2.

Any request for IT data will be formally requested by the HR & Transformation Manager, after taking consideration of the nature and severity of the alleged misconduct and the grounds to request such data. On no account should operational managers contact ICT Services direct for access to information.

Any request for door access data should be formally requested by the HR & Transformation Manager to the Facilities Manager.

If any such records are used in a formal disciplinary case, then the use of such records should be reasonable and proportionate to the case. All records should be kept secure and destroyed at the conclusion of the case (allowing for the time period to expire for appeals and employment tribunal claims).

8.4 **Covert monitoring**

Covert monitoring (carrying out monitoring in secret without staff being told they are being monitored) is rare but may be considered necessary when employers have a genuine reason, such as criminal activity or equivalent malpractice. Covert monitoring is strictly covered by the Regulation of Investigatory Powers Act and advice must be sought from the Legal Manager or the HR & Transformation Manager in the first instance.