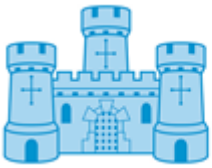

NEWCASTLE·UNDER·LYME
BOROUGH COUNCIL

CCTV POLICY

FEBRUARY 2020

Contents

1. Introduction

1.1. This Policy governs the operation of the closed circuit television (CCTV) systems operated by Newcastle-under-Lyme Borough Council as a data controller to assist it in carrying out its enforcement, public safety and other functions.

1.2. The Council uses Closed Circuit Television (CCTV) systems in public spaces, within car parks, on some Council vehicles and at a number of Council owned sites across the Borough.

1.3. This document along with individual systems Codes of Practice are designed to give clear guidelines on the Council's use of CCTV and to protect the Council and its CCTV operators from allegations of misuse of the system and to protect staff and the public from any abuse of the CCTV system.

1.4. This Policy covers the use of CCTV equipment and the gathering, storage, use and disposal of visual data. This Policy applies to all staff employed by Newcastle-under-Lyme Borough Council and should be the standard expected from any external agencies or persons who operate CCTV systems on its behalf.

1.5. The Policy sets out the principles to be observed by the Council, its members, employees, contractors, and any other parties or organisations involved in the operation, management and administration of relevant CCTV systems, as well as the hierarchy of responsibilities which exist to ensure that these systems are operated in a compliant manner.

1.6. However it is also intended to inform members of the public of the purposes for which CCTV is operated, and of the standards which will be met in relation to it. In this way, the Council can be held accountable for its compliance with the Policy.

1.7. A list of key definitions and acronyms is set out at Section 12 of this document.

1.8. The Policy is supplemented by Procedures and a checklist for Council departments to follow when procuring and installing CCTV systems.

1.9. This Policy does not govern the Council's use of the surveillance powers available to it, which are conducted under the auspices of the Regulation of Investigatory Powers Act. Covert surveillance is governed by a separate document, the Council's RIPA Policy.

1.10. This document should be read in conjunction with the Staffordshire Police and Local Authority External CCTV Partnership Policy, Procedures and Strategy. Failure to comply with these documents could lead to disciplinary action, which may lead to dismissal and in certain circumstances criminal proceedings against the individuals concerned.

2. Proportionate Response

2.1. Compliance with this Policy and with the detailed arrangements which sit under it ensures that the Council's use of CCTV cameras reflects a proportionate response to identified problems, which is operated with due regard to the privacy rights of individuals.

3. Purpose of CCTV

3.1. It is important that everyone and especially those charged with operating the CCTV systems on behalf of Newcastle-under-Lyme Borough Council understand exactly why each of the systems has been introduced and what the cameras will and will not be used for. The principle is that CCTV will only be considered where alternative options to resolve issues have been discounted.

3.2. Each CCTV system will have its own site or task specific purposes objectives. These will include some or all of the following:

- Protecting areas and premises used by Council staff and the public;
- Protecting the safety of the public using Council facilities;
- Deterring and detecting crime and anti-social behaviour;
- Assisting in the identification of offenders leading to their arrest and successful prosecution or other appropriate action;
- Reducing violent or aggressive behaviour towards staff;
- Reducing fear of crime, anti-social behaviour and aggression;
- Protecting Council property and assets;
- Maintaining and enhancing the commercial viability of the Borough and encouraging continued investment;
- Assisting in Planning Enforcement;

3.3. The CCTV systems may also be used to inform internal disciplinary investigations, grievance, formal complaints and Health and Safety Investigations where appropriate in. This may be in response to an incident or following checks.

4. Background

4.1. In recent years there has been a substantial increase in the number of CCTV cameras, driven in part by increasing concerns for personal and property safety and security. This increase has coincided with heightened privacy concerns, which have resulted in laws, regulations and codes of practice designed to ensure that the use of cameras is legitimate, proportionate to the intended purpose and respectful of the legitimate privacy expectations.

4.2. Article 8 of the Human Rights Convention recognises the right to a private and family life. Where CCTV captures images of people which comprise personal data, there is potential for this to infringe on the privacy of individuals. Accordingly, there is an obligation for CCTV installations and handling practices to comply with the 3rd Data Protection Principle (data minimization) as well as the 6th Principle (Appropriate technical and organisational security).

4.3. CCTV systems are operated by the Council and its partners only as a proportionate response to identified problems, this in so far as it is considered necessary in a democratic society in the interests of public safety, for the prevention and detection of crime and disorder and for the protection of the rights and freedoms of others.

4.4. The Information Commissioner's Office ('the ICO') has enforcement powers which include the power to issue directives to remove or modify CCTV installations. The ICO is supported by the Surveillance Camera Commissioner, which was established under the Protection of Freedoms Act 2012 and has issued a codes of practice for the use of these cameras, which includes the guiding principles set out below.

5. Scope of This Policy

5.1. The Council acts as data controller for the CCTV systems it operates for the purposes of maintaining preventing and detecting crime and for ensuring public safety, including that of attendees at its public venues. The scope of this policy includes the following CCTV types:

a) *Fixed CCTV Systems*
Fixed CCTV systems are those which are installed permanently with cameras in fixed locations. This may be within a building or an external location, such as the town centre. There are a number of locations where fixed CCTV is in operation, see Appendix B for further details.

b) *Re-deployable CCTV*
Re-deployable CCTV (RCCTV) shares many of the attributes of Fixed CCTV but the entire system can be moved and fixed in a new location, should monitoring requirements change.

It is ideal for providing temporary monitoring and security for short-term applications such as investigating criminal activities such as fly tipping and events. It can be installed quickly and at a significantly reduced cost linking to existing infrastructures. Re-deployable CCTV cameras are occasionally used by the Council and must comply with the requirements set out in this Policy Document.

c) *Mobile CCTV*
Mobile CCTV describes single or multiple cameras fixed to a vehicle or other moving object. Many of the Council's vehicles are equipped with CCTV recording systems, such as Recycling and Waste and Streetscene vehicles which have multiple cameras for the purposes of staff and public safety. These systems may also be used for providing evidence for insurance claims.

Drones or other aerial platforms used for the purpose of gathering video imagery may also be considered as mobile CCTV and must be compliant with this policy.

d) *Body Worn Cameras*
Some staff or contractors particularly with public enforcement roles wear body-mounted cameras to protect their safety and wellbeing whilst carrying out their duties. Body worn cameras have the potential to capture imagery and audio in considerably closer proximity than typical fixed, re-deployable or mobile CCTV systems.

The privacy impact associated with the use of body-worn cameras is significant and the subsequent storage and processing of captured data must be given particular consideration and appropriate guidance must be provided to staff and contracts regarding the system's use.

e) *Automatic Number Plate Recognition (ANPR) Systems*
ANPR systems can operate in both fixed and re-deployable situations and are typically used to capture identification numbers from vehicles passing through a particular point. Such systems are typically used in car parks for purpose of charging, but also have potential use at the roadside for enforcement and monitoring activities, or at temporary events for security purposes.

Whilst ANPR systems will not directly collect personally identifiable information in isolation, they must still fully comply with this policy.

f) *Drones*
The Council does not currently utilise drones however should aerial footage be used in the future this will be subject to this policy and a PIA.

6. General Principles/ Guidelines

6.1. The Council's use of CCTV accords with the requirements and the principles of the Human Rights Act 1998, the General Data Protection Regulation ((EU) 2016/679), the Data Protection Act 2018 and the Protection of Freedoms Act 2012.

6.2. This Policy recognises the need for formal authorisation of any covert 'directed' surveillance as required by the Regulation of Investigatory Powers Act 2000, and provides that CCTV shall be operated fairly, within the law and only for the purposes for which it was established or which are subsequently agreed in accordance with the Code.

6.3. CCTV shall be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and home. Public interest in the operation of CCTV will be recognised by ensuring the security and integrity of operational procedures which sit underneath it, and which balance the objectives of the CCTV usage with the need to safeguard the individual's rights.

6.4. This Policy ensures that CCTV used by or on behalf of the Council is:

a) *Transparent*
Wherever possible, the presence of CCTV, the purpose for it and contact details for the Controller of it should be clearly displayed to the public and staff.

There are strict laws around the use of covert surveillance cameras and these should only be implemented where necessary for a criminal enforcement purpose where the Council has the necessary statutory authority and under the oversight of the Senior Information Officer.

b) *For a Legitimate and Specified Purpose*
Prior to establishing any CCTV installation, it is necessary to establish a legitimate purpose for it. The appropriate balance between the necessity of the CCTV and the privacy rights of individuals can only be assessed in light of this intended purpose.

c) *Proportionate to That Purpose*
The usage of CCTV cameras, including the field of vision and whether they can be controlled remotely, has to be proportionate to the identified need. For example, installation of a camera for the purpose of public safety would be unlikely to be proportionate in an area with no particular history of incidents.

Subject to a review of the balance to be drawn between personal privacy and the wider public interest, the Council will explore opportunities to utilise Artificial Intelligence technologies in conjunction with CCTV recordings.

The Council will also consider the use of aerial CCTV recording platforms such as drones. Where external operators are engaged, the Council will seek where possible to ensure they are approved as part of the Surveillance Camera Commissioner's third party certification scheme.

d) *Privacy Impact Assessed*
All existing and proposed CCTV installations should be subject to a Privacy Impact Assessment (PIA) to identify what risks to privacy (for both staff and members of the public) they pose and what controls can be applied to minimize these.

e) *Subject to Senior Management Approval and Oversight*
Proposals to install CCTV must be considered by the Information Governance Group and approved by a member of the Executive Management Team. Where a privacy impact assessment indicates a high risk, the approval of the Senior Information Risk Officer (SIRO) is required prior to the procurement of CCTV equipment.

f) *Secure From Inappropriate Access and Interference*
As CCTV recordings contain personal (and sometimes special category) data, there is a legal obligation to ensure that access is limited to those with a genuine need and that any data held meets appropriate technical standards for information security. The Information Governance Officer will have such access rights. In the event of a data breach, prompt steps must be taken in accordance with the Council's procedures to mitigate the breach and to notify relevant parties.

g) *Subject to Clear and Binding Operational Procedures*
All Council departments operating CCTV are required to ensure that there are procedures in place which regulate where cameras can be installed, where they should point, under what circumstances data can be accessed or removed from the devices and under what circumstances in can be disclosed to other parties.

These procedures should be clear and binding for all staff and contractors with responsibilities for operating or managing CCTV. Failure to abide by operational procedures may be subject to disciplinary action.

h) *Auditable*
All staff actions which effect the operation of CCTV equipment should be captured in audit logs held on the devices or controlling applications. This includes any actions which change the field of vision, any downloads of footage and any deletion of footage. All CCTV equipment must be specified so as to provide accurate time and date stamping,

All CCTV installations will be recorded on the Council's CCTV Register.

i) *Subject to Data Retention Processes*
CCTV systems operated by the Council shall normally retain footage for no longer than 30 days. Where footage is required for the purposes of prosecution of an offence or to defend legal claims or to inform internal investigation, where appropriate a copy should be made and stored securely with controlled access to appropriate personnel.

j) *Subject to a Defined Data Sharing Process*
The Police, social services, environmental health and/or other authorised agencies or bodies may apply for access to data collected via CCTV in order to carry out their statutory functions. All requests will be reviewed by the Council's Information Governance Officer and determined according to a process which ensures requests are reasonable and comply with the law.

The Council commission's third parties to undertake some of the CCTV functions, in these circumstances the commissioned services should comply with the principles of this policy.

7. Surveillance Camera Code of Practice

7.1. This Policy is based on the 12 guiding principles set out in the Surveillance Commissioner code of conduct:

I. Use of a CCTV system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

II. The use of a CCTV system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

III. There must be as much transparency in the use of a CCTV system as possible, including a published contact point for access to information and complaints.

IV. There must be clear responsibility and accountability for all CCTV system activities including images and information collected, held and used.

V. Clear rules, policies and procedures must be in place before a CCTV system is used, and these must be communicated to all who need to comply with them.

VI. No more images and information should be stored than that which is strictly required for the stated purpose of a CCTV system, and such images and information should be deleted once their purposes have been discharged.

VII. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

VIII. CCTV system operators should consider any approved operational technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

IX. CCTV system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

X. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

XI. When the use of a CCTV system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

XII. Any information used to support a CCTV system which compares against a reference database for matching purposes should be accurate and kept up to date.

8. Legislation

8.1. In addition to Council Policies, Procedures and guidelines, CCTV and its operation are subject to legislation under:

a) The Data Protection Act 2018 (DPA).

b) The Human Rights Act 1998 (HRA).

c) The Freedom of Information Act 2000 (FOIA).

d) The Regulation of Investigatory Powers Act 2000 (RIPA).

e) The Protection of Freedoms Act 2012

f) General Data Protection Regulations (GDPR)

g) Computer Misuse Act (CMA)

8.2. General guidance can be found in the Information Commissioner's Office (ICO) CCTV Code of Practice (available at www.ico.org.uk) and the Surveillance Camera

Commissioner website, to encourage compliance with the surveillance camera code of practice; https://www.gov.uk/government/collections/surveillance-camera-guidance-tools-and-templates.

8.3. It is important that the operation of all Council CCTV systems comply with these Acts, Policies, Procedures, Guidelines and Codes of Practice.

9. Roles and Responsibilities

9.1. All staff with operational access to CCTV equipment are responsible for following the specific operational procedures established for its use. This includes checking the equipment and reporting to management where it is found to deviate from the agreed specification or appears to have been interfered with.

9.2. Responsible Officers (ROs) are accountable for identifying a legitimate need for CCTV installations where one exists (and for reviewing the same), for ensuring that data privacy impact assessments are conducted and an action plan generated and progressed and for making sure that risk controls are established where needed to protect personal privacy. A list of CCTV locations and ROs can be found at Appendix B.

9.3. The ROs are responsible for the day-to-day operation of the CCTV system within their charge and the security and accountability of all equipment and media used by their system. This includes any system owned by the Council but which is managed by a third party. In some circumstances the Council will lease out commercial properties that have CCTV, the responsibility for these systems transfer to the tenant.

9.4. Making sure that authorised staff, their operating team and people authorised to view images using the CCTV system are properly trained in the use of the equipment and comply with the Policies, Procedures and Guidance. They are not to permit any other staff to operate the equipment or view images without authorisation.

9.5. The Information Governance Group are responsible for approving proposed new CCTV installations and any significant changes to existing ones. Where proposed installations are assessed as posing a high risk to personal privacy, they are responsible for referring the matter to the Senior Information Officer (SRO) for approval.

9.6. The SIRO is responsible for setting the risk appetite for CCTV installations for the Council and assessing high risk proposals as referred. This will be done in conjunction with the Information Governance Group.

9.7. The Information Governance Officer (IGO) is the Council's Single Point of Contact (SPOC) and is responsible for assessing proposed CCTV installations posing a high risk to privacy, rights and freedoms and for making recommendations to the SRO. In cases of a serious breach involving CCTV data, the DPO is responsible for reporting the matter to the ICO.

9.8. The Information Governance Officer is responsible for maintaining the Corporate CCTV Register, assisting departments with Data Privacy Impact Assessments and participating in the investigation of breaches.

9.9. Where the Council receives CCTV footage from a third party the relevant officers will ensure that they comply with this policy and that data is treated securely. Officers should seek advice from the Information Governance Officer.

10. Data Protection and subject access rights

10.1. Residents and staff have the following rights with regard to CCTV footage captured by the Council's cameras:

a) A right to request through subject access, a copy of footage in which they are captured, subject to exemptions within the Data Protection Act 2018 and also balanced against the rights and freedoms of others who may appear in that footage. A Subject Access Request Form can be found on the Council's website.

b) A right to object to processing where they believe that the field of vision or the siting of the camera is disproportionate to the stated purpose of the camera. Where a resident objects to processing, the Council will consider the objection and decide whether a lawful basis for processing can still be justified. A written response will be provided outlining the outcome. Objections can be raised by writing to: dataprotection@newcastle-staffs.gov.uk

11. Data Retention & sharing

11.1. All Council CCTV Cameras automatically over-write footage between 28 and 31 days after it is captured. Requests for data will be directed through the Single Point Of Contact and the request form will ask for information on the person requesting the information to ascertain that they have the legal justification for the data. Where authorized bodies are granted access to data collected via CCTV in order to carry out their statutory functions, then copies of the data may be made and provided securely for this purpose.

12. Key Definitions and Acronyms

CCTV	Closed Circuit Television
Data Protection Officer (DPO)	A statutory role set out under the Data Protection Act with responsibility for ensuring that organisations are compliant with personal privacy rights. Any resident can report a personal privacy concern about the Council to the Data Protection Officer. The role of the Data Protection Officer is within the remit of the Council's Information Governance Officer
Single Point Of Contact (SPOC)	First and single point of contact for all matters in relation to surveillance cameras.
General Data Protection Regulation (GDPR)	Regulations establishing data protection principles and privacy rights for people whose data is processed in the European Union. It is supplemented in British law by the Data Protection Act 2018 which enshrines its rights and principles.
Responsible Officers (RO)	A role held by a senior manager at the Council, to ensure that information systems operated by their teams have appropriate data quality, auditability and access controls.
Information Governance	The discipline of applying controls to how information or data is created, how it is stored and where it moves.
Senior Information Risk Officer (SIRO)	A role established under International Information Security Standard ISO27001 to ensure that appropriate processes for information risk and the treatment of that risk are established and maintained. At the Council, the

	role is held by the Executive Director of Finance & Resources.
The Regulation of Investigatory Powers Act 2000 (RIPA)	This act sets out the conditions under which investigations and covert surveillance can be lawfully conducted.
Overt Surveillance	Examples of this include; • Police Officer or Parks Warden on patrol • Sign-posted Town Centre CCTV cameras (in normal use) • Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. • Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert Surveillance (but not requiring prior authorisation)	Includes CCTV cameras providing general traffic, crime or public safety information.
Directed Surveillance (must be RIPA authorised in line with the Council's RIPA Policy)	Examples of this include; • Officers following an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long term sick from employment. • Test purchases where the Officer has a hidden camera or other recording device to record information that might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.
Intrusive Surveillance	THE COUNCIL DOES NOT HAVE A LAWFUL BASIS TO CARRY OUT THIS TYPE OF ACTIVITY. Examples of this include planting a listening or other device (bug) in a person's home or in their private vehicle.

13. Review of this Policy

13.1. This Policy will be reviewed annually under the oversight of the Senior Information Officer.

14. Related Policies

14.1. Data Protection Policy – June 2019

14.2. RIPA Policy – February 2019

15. Appendices

15.1. Appendix A) Privacy Impact Assessment

15.2. Appendix B) Deployment of CCTV Systems and Responsible Officers (ROs)

Appendix A CCTV Privacy Impact Assessment

The document should be completed prior to any project commencing and should be updated throughout the course of a projects life.

Name (person completing the form)	
Position	
Responsible Officer	
Position	
Service Area and Department	
Date of completing form	

Please Note: Some or all of the information provided in this document may be subject to disclosure and/or publication under the Freedom of Information Act 2000.

CCTV System Location and Purpose
Describe the location, type and purpose of the CCTV system. For example: *Midway Carpark* *Fixed CCTV Installation* *Security of Council property and safety of car park patrons.*
Identify the need for a Privacy Impact Assessment
The CCTV system proposed for / located at [INSERT LOCATION] will result in: • The collection of new information about individuals • Individuals will be indirectly and indiscreetly compelled to provide identifying information through the capture of their image. • Information may be disclosed to organisations or people who have not previously had routine access to the information. • CCTV systems may involve the use of new technology which might be perceived as being privacy intrusive. • Captured data may result in the making of decisions or the taking of action against an individual in ways which may have a significant impact on them. • The information may be of a kind particularly likely to raise privacy concerns or expectations.
Describe the information flows
The collection, use and deletion of personal data should be described. You may want to refer to a flow diagram to explain the data flow. You should say how many individuals are likely to be affected by the CCTV system (i.e. footfall through a building).

Collection of Data

Fully describe how data will be collected. You should include reference to a diagram of where cameras are situated which each point clearly located. For each point, you should complete a relevant entry in the camera details table as shown below.

Camera Reference	*Reference to the location on the diagram*
Camera Location	*Describe the Camera location (for example, ceiling mounted)*
Public Area	*Is the camera likely to capture indiscreet images of members of the public?*
Camera Type	*Include details of the camera type and capabilities (such as colour or mono, operating resolution, multi-directional or fixed, audio capable or mute, etc.)*
Communication Method	*How is the camera connected to the controller, for example Wired IP, Wi-Fi, 4G, Coaxial, Optical, Twisted Pair, etc.*
Specific Considerations	*For example, "The cameras field of view includes the entrance of a changing area but does not cover inside the changing area"*

(Copy and Paste as many of the above tables as required for each camera)

Fully describe the data recording and retrieval system:

Manufacturer	*For the storage and control system*
Model	*For the main control unit*
Media Type	*For example, hard drive, tape, DVD-RW, Network Storage*
Media Storage	*If the storage media is removable, how is this kept secure? For example, media cards are encrypted and stored in a locked cabinet. The storage device is bolted to the wall/cabinet.*
Export Capability	*For example, record to DVD, export to memory stick*
Data Encryption	*Does the system encrypt data when it is stored (at rest)?*
Export Encryption	*Can data exported from the system be encrypted?*
Authentication Method	*Describe any authentication methods in place to ensure the system can only be accessed by appropriate personnel*
Role Specific Authentication	*Describe how the system ensures that only authorised personnel can use the system for playback, export, configuration, etc.*
Auto Date/Time Update	*Is the date and type recorded on the system automatically updated and if so, what is the source?*
Retention Period	*How long is the system set to keep information?*
Automated Deletion	*Does the system automatically remove data after a fixed period?*
Control Interface	*Fully describe the systems main control interface (or interfaces), its location and capabilities. For example, a dedicated control pad is located in a secure area. It can be used to pan and rotate cameras, view live images, playback and export stored information.*
Playback Interface	*Fully describe any playback interfaces and where they are located. For example, a 32" LCD screen displays live camera feeds from 4 locations and behind the reception desk.*
Publicly Viewable Controls	*Yes / No – are any playback facilities visible to members of the public during the systems standard operation (i.e. a display behind reception).*
Remotely Accessible	*Are the system controls remotely accessible, such as through the use of a network interface, control software, etc. You should indicate if the system has the capability for remote accessibility, even if it is not in use.*
Camera Communications	*Describe the method used for cameras to communicate with the controller. For example, this may be IP communications for modern systems. Older systems may use Coaxial or Component video.*

Consultation requirements
Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? For the purpose of this assessment you may include details of how you will inform individuals the CCTV is in operation. For example, it would not be possible to consult every individual entering a site before their image is captured by CCTV. However, clear signage would indicate the present and purpose of a CCTV installation.

Identify the Privacy and Related Risks

Identify the key privacy and corporate risks. Compliance risks will be completed by Information Governance Group.

Privacy risk	**Risk to individuals**	**Compliance risk**	**Associated organisation/corporate risk**
E.g. Intrusion of privacy, data loss, unauthorised use of data	E.g. Unable to use service, damage and/or distress, risk of physical harm	E.g. Breach of GDPR, HRA, Confidentiality	E.g. Regulatory action, reputational damage, loss of trust

Identify Privacy Solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary, e.g. the production of new guidance or future security testing for systems.

Risk (as identified above)	**Solution(s)**	**Result**
	E.g. training, policy update, agreement/contract NB: There may be more than one possible solution for each risk	Is the risk eliminated, reduced or accepted

Sign off and record the PIA outcomes

Who has approved the privacy risks associated with the CCTV system? Which of the solutions identified above need to be implemented?

Risk (as identified above)	**Approved solution**	**Approved by**

Integrate the PIA outcomes back into the CCTV plan *Who is responsible for integrating the PIA outcomes back into the CCTV plan and updating any operational processes? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?*		
Action to be taken	**Date for completion of actions**	**Responsibility for action**

What happens next?

Please return your completed Privacy Impact Assessment form to the Information Governance Group.

The assessment will be reviewed, and the group will:

1. Identify any additional risks and solutions which the service may not have identified.

2. Identify where there may be areas of non-compliance with statutory and regulatory requirements and any further risks that this may have on the individual/organisation.

3. Return the Assessment to you, along with any recommended changes, for acceptance of those changes and approval/sign off.

Once the Assessment has been approved, a final approved copy should be provided to the Information Governance Group so that this can be recorded and published. The service will then be responsible for implementing any of the agreed solutions and actions.

Appendix B Responsible Officers

Location and CCTV Type	Responsible Officer
Depot (3 sites), Fixed CCTV Refuse Freighters, Mobile CCTV	Head of Fleet & Recycling Services
Streetscene Vehicles, Mobile CCTV	Head of Operations
Town centre, Fixed CCTV	Head of Housing, Regeneration and Assets Services
J2, Fixed CCTV	Head of Leisure & Cultural Services
Museum, Fixed CCTV	Head of Leisure & Cultural Services
Kidsgrove Town Hall, Fixed CCTV	Head of Customer and Digital Services
Enforcement Officers, Body Worn CCTV Environmental Health Enforcement Team, Body Worn and Re-deployable CCTV	Head of Environmental Health
Midway Car Park, Fixed CCTV	Head of Housing, Regeneration and Assets Services
Keele Cemetery, Fixed CCTV Crematorium, Fixed CCTV	Head of Operations
Housing Services Mobile CCTV	Head of Housing, Regeneration and Assets Services