CCTV and Directed Surveillance Policy

1. Purpose

The purpose of this Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) systems at the academies within The Talentum Learning Trust (TTLT). This policy details the procedures to be followed to ensure that the Trust and its academies comply with relevant legislation and codes of practice for processing data captured through use of CCTV systems. This policy will be subject to review annually to include consultation as appropriate with relevant parties.

2. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- The UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998
- Children Act 1989
- Children Act 2004
- Equality Act 2010

This policy operates in conjunction with the following statutory and non-statutory guidance:

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2022) 'Video Surveillance'

This policy operates in conjunction with the following Trust policies:

- Freedom of Information Policy
- Data and Cyber Security Breach Prevention and Management Plan
- GDPR Privacy Notices

- Data Protection Policy

3. Objectives of the CCTV Policy

- To increase personal safety of staff, pupils/students and visitors and reduce the fear of crime;
- To protect TTLT buildings and their assets;
- To support the police in a bid to deter and detect crime;
- To assist in identifying, apprehending and prosecuting offenders;
- To assist in managing the academies and the investigation of suspected breaches of Academy/Trust regulation;
- To help ensure that those capturing individuals' information comply with the DPA 2018, UK GDPR and other such relevant statutory obligations;
- To contribute to the efficient deployment and operation of a camera system;
- To ensure that the information captured is usable and can meet its objectives in practice;
- To reduce reputational risks by staying within the law and avoiding regulatory action and penalties;
- To re-assure those whose information is being captured, of Academy compliance.

4. Statement of intent

Surveillance camera systems are deployed extensively within the UK and where they are used appropriately, these systems are valuable tools which contribute to public safety and security and in protecting both people and property. The Trust and its academies seek to operate CCTV systems in a manner that is consistent with respect for the individual's privacy.

The majority of surveillance systems are used to monitor and/or record the activities of individuals and as such they process individuals' personal data. Most uses of surveillance systems will therefore be covered by the Data Protection Act 2018 and the UK GDPR, and the provisions of the ICO's codes of practice for the use of CCTV systems and surveillance.

Using surveillance systems can be privacy intrusive. They are capable of placing large numbers of law-abiding people under surveillance and recording their movements as they go about their day-to-day activities. As such, academies will carefully consider whether or not to use a surveillance system and will take into account the nature of the problem they are seeking to address, inclusive of:

- Whether a surveillance system would be a justified and effective solution
- Whether better solutions exist
- What effect its use may have on individuals, and whether in the light of this, its use is a proportionate response to the problem

As such, TTLT and the academies will treat the systems and all information, documents and recordings obtained and processed as data which are governed by the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). Cameras will be used to monitor activities within Academy premises; buildings, car parks and other such public areas to identify criminal activity

actually occurring, anticipated, or perceived, and for the purpose of ensuring the safety and wellbeing of Academy staff, pupils/students and visitors, alongside the security of the premises.

The planning and design has endeavoured to ensure that the CCTV will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

The use of CCTV systems in academies will be regularly reviewed for effectiveness in accordance with their original purpose for siting. Cameras in situ will be subject to review at least on an annual basis. CCTV which is not utilised for its original purpose in accordance with section one of this policy, or which is no longer effective, may be subject to decommission following reviews of usage.

It should be noted that CCTV is not utilised in all TTLT Academy buildings and external premises and therefore this policy only applies to those academies who operate CCTV systems.

5. Operation of the system

This policy will be administered and managed by the Headteachers or their nominee, in accordance with the principles and objectives expressed in this policy and the relevant data protection laws. The day-to-day management will be the responsibility of the Senior Leadership Teams (SLT), ICT Technicians and the Premises Managers. The CCTV system is capable of being operated for 24 hours per day, every day of the year.

Systems in place comprise of a number of fixed cameras located around Academy premises where there is a legitimate requirement for such monitoring in accordance with the purpose limitation principle of the UK GDPR; 'personal data should be collected for specific and legitimate purposes and must not be further processed in a way which is incompatible with such purposes.'

In accordance with the Surveillance Camera Code of Practice, CCTV System operators should adopt the following guiding principles:

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints, these are available on the Trust website, through the Trust Privacy Notices.
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
- Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
- 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.

- Surveillance camera 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.
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use, both physically and technically.
- 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.
- When the use of a surveillance camera 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.
- Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Camera footage can **only** be reviewed by designated staff (Academy employed IT Technicians, Premise Managers and Senior Leadership Teams) in accordance with the integrity and confidentiality principle of the UK GDPR, to ensure that all personal data is maintained on a confidential basis, is secure against unlawful processing, accidental loss or disclosure, destruction or damage.

The CCTV systems will be used to observe Academy premises and areas under surveillance in order to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

Staff are instructed that static cameras are not to focus on private homes, gardens and other areas of private property. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained using the Academy's forms for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

Classroom footage will not be used for the purposes of staff Performance Management, capability or disciplinary action. Any CCTV cameras deemed necessary for installation in classrooms must undergo a data protection impact assessment and consultation with the DPO, followed by contact with the ICO and relevant Unions as necessary, before being installed. CCTV will only be used for the objectives outlined in section three of this policy.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Footage will only be released to the media for use in the investigation of a specific crime and with the written authority of the police and following consultation with the CEO, DPO and ICO as necessary to conform with the principles of data protection in accordance with the UK General Data Protection Regulation and Data Protection Act 2018. Footage will never be released to the media for purposes of entertainment. Compliance with the UK GDPR will be maintained for use of CCTV systems.

Each Academy that houses CCTV must have a map of the locations of each camera installation, to support in monitoring and reviewing the purpose of each sited camera. The system should be maintained to permit optimum performance and address functionality issues.

Warning signs notifying premise users of the presence of CCTV, as required by the Code of Practice of the Information Commissioner must be placed at all access routes to areas covered by CCTV.

Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with TTLT policies and procedures and be authorised by the CEO.

6. Monitoring procedures

Camera surveillance must be maintained at all times; where staff are not monitoring the system, the system should be locked or made otherwise inaccessible to unauthorised personnel. CCTV must not be controlled by unauthorised personnel and screens used to view footage must not be accessible or viewable by those who do not have authorisation to do so. Pictures will be continuously recorded and CCTV systems cannot be accessed remotely.

Recorded images must be viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where an individual would have an expectation of privacy should be restricted to authorised persons as mentioned in section one of this document. Where images are in an area of particular sensitivity, it may be more appropriate to only view recorded images after an incident has occurred.

CCTV should only be accessible through password protected and suitably encrypted devices. Passwords must be changed on regular basis in line with the Trusts Data and Cyber Security Breach Prevention and Management Policy, be of suitable length and with a variety of characters and numbers, i.e. at least eight characters of upper and lower case and at least one number.

Images are recorded on servers located securely in each Academy. Server rooms must be secure and accessible only to authorised members of staff. Additional staff may be authorised by the Headteacher to temporarily monitor cameras sited within their own areas of responsibility, provided that the footage is viewed purely for the purposes defined in section one of this policy and on a view only basis. All staff must adhere to the code of conduct and maintain strict confidentiality when viewing CCTV.

Server rooms and the facilities/assets contained within them will be subject to regular maintenance by external contractors. Academies must ensure that CCTV systems are appropriately locked and secure to ensure that the information within these systems remains inaccessible to unauthorised parties, and that contractors are inducted to site security accordingly to ensure that they are aware of their obligations to ensure system security and confidentiality is maintained.

Cameras are monitored in designated rooms, circulations and external areas of each Academy, which are a secure area and staffed during working hours. Damage is reported to appropriate staff. The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are checked and maintained at regular intervals to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

All images recorded by the CCTV System remain the property and copyright of the Trust, and CCTV systems themselves are owned by the Trust. The monitoring of staff, pupil/student and visitor activities will be carried out in accordance with Trust policies and practices.

7. Installation of New Systems and the Addition of Cameras

Any proposed new CCTV installation is subject to a Data Protection Impact Assessment and must be able to demonstrate a clear purpose to protect the Academy building(s) and/or occupants.
Any proposed additions to existing CCTV installations are subject to a Data Protection Impact Assessment and must be able to demonstrate a clear purpose to protect the Academy building(s) and/or occupants.
Consultation with the DPO is required for new installations and the addition of cameras.

8. Review of System Usage

The use of each CCTV system should be reviewed on at least an annual basis for effectiveness and to ensure that the system fulfils the purpose for which it was originally installed.
Appendix B of this policy should be utilised to perform the review.
The siting of each camera on the system must be reviewed, alongside the system as a whole.
Cameras which are deemed ineffective or can no longer be utilised for the purposes they were original installed will be decommissioned accordingly.

9. Compliance with Data Protection Legislation

In administration of CCTV systems, academies must ensure that they comply with the UK GDPR and follow Trust policies for Data Protection and Records Management. The principles of the UK GDPR define that personal data shall be;

- Processed lawfully, fairly and transparently;
- Collected for specific, explicit and legitimate purposes in accordance with the purpose limitation principle;
- Limited in processing to what is necessary to fulfil the purpose for which it was collected;
- Accurate;
- Kept in a form which permits identification of data subjects for no longer than is necessary to fulfil processing purposes;
- Subject to appropriate security measures, including protection against unauthorised or unlawful processing against accidental loss, destruction or damage, using suitable organisational measures in order to meet the principle of confidentiality and integrity;
- Maintained in accordance with the accountability principle. Academies utilising CCTV maintain the responsibility for ensuring compliance with data protection laws.

Any and all uses of CCTV systems must be in accordance with relevant data protection legislation; academies and their staff who utilise such systems must protect the personal data contained both in electronic storage systems and through live footage by:

- Keeping the data in a form which identifies individuals for no longer than the specified retention period unless there are compelling legal reasons to do so, such as the footage will be utilised as part of criminal proceedings in a court of law;
- Be used only to collect data for the purposes outlined in section one of this policy; mainly to safeguard staff, pupils and visitors on the premises from crime and to act as both a deterrent to crime and an aid in prosecution where the deterrent has not been successful;

- Informing individuals about the usage of CCTV on the premises through appropriate signage and privacy notices;
- Be positioned in places which comply with the purposes for which the cameras are being used;
- Regularly reviewing the effectiveness of the system, and the requirements for CCTV.

Any proposed deployment that includes audio recording in a public place is likely to require a strong justification of necessity to establish its proportionality. There is a strong presumption that a surveillance camera system must not be used to record conversations as this is highly intrusive and unlikely to be justified. Any proposed deployments of this nature must first be consulted with the CEO and DPO.

Any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose, and be suitably validated. Any proposed deployments of this nature must first be consulted with the CEO and DPO.

Changes in the use of systems must be reflected in Academy privacy notices.

10. Access by the Data Subject

The General Data Protection Regulation provides Data Subjects (individuals to whom "personal data" relate) with a right of access to data held about themselves, including those obtained by CCTV. Where a request for access is made, this is called a Subject Access Request (SAR). SARs must be made to the Trust DPO. In practical terms, if individuals are capable of being identified from the relevant surveillance system, then it is classified as personal information about the individual concerned.

In order to locate images on the Academy's CCTV system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject found, defined as the scope of the request. Academies who receive a SAR of this nature must follow TTLT's procedure for handling Subject Access Requests and consult with the DPO prior to providing personal information. The Academy and DPO may consider that it would be more suitable for the individual to attend site to view the footage, rather than providing a copy.

TTLT will protect the rights of third parties whose images may also be captured on the CCTV footage requested by obscuring their identity as far as reasonably practical. Where the Academy is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it must consult with the DPO prior to releasing any information. The Academy may not be obliged to comply with the request unless satisfied that the third party has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the third party or that reasonable measures can be taken to protect the identity of the individual, without having their consent for release of data as per the SAR. Consultation will be undertaken with the ICO as deemed necessary by the DPO in accordance with the request.

A request for images made by a third party (SAR) should be made in writing to the Trusts DPO. Data requested as part of a SAR will not be released until the DPO has satisfactorily verified the identity of the individual and followed the Subject Access Request procedure. Data that can be released in compliance with the law, will be released within 30 days of the request, or 90 days where there are exceptional circumstances. The Academy must consider whether the data will be removed from the system before the SAR can be fulfilled, in order to preserve it e.g. the system holds CCTV data for 30 days but the individual

has made a request on day 15 and the Academy therefore needs to continue to hold the data through following the SAR procedure.

In limited circumstances, it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation. Such disclosures will be made in conjunction with the DPO and ICO (where relevant) with reference to applicable legislation and in accordance with section 6 of this policy.

The Academy may provide access to CCTV images to Investigating Officers when sought as evidence in relation to student disciplinary cases or staff human resource cases, and where they have obtained the consent of the individual in order to do so, where consent is required in accordance with the nature of the individual case. This is upon approval of the CEO.

A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure. Any copied CCTV footage will be subject to suitable encryption methods before being released.

11. Third party access

In order to maintain and preserve the integrity of the disks or other portable devices (such as USB drives or hard drives) used to record events from the hard drive, store data and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- Each disk/portable device containing personal identifiable information in the form of CCTV footage must be identified by a unique mark **and encrypted prior to release.**
- Before using each disk/portable device must be cleaned of any previous recording.
- The Academy shall register the date and time of the disk/portable device insert, including reference.
- A disk/portable device required for evidential purposes must be sealed, witnessed, signed by the Academy, dated and stored in a separate, secure, evidence disk store. If a disk/portable device is not copied (if required for copy) for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence disk/portable device store.
- If the disk/portable device is archived the reference must be noted, and the purpose for archiving must be recorded.
- Disks/portable devices containing footage may be viewed by the Police for the prevention and detection of crime and authorised officers of TTLT for supervisory purposes.
- A record will be maintained of the release of disks to the Police or other authorised applicants as part of the procedure for releasing data for a Subject Access Request. A register will be available in each Academy for this purpose.
- The viewing of disks/footage located on portable devices by the Police must be recorded in writing. Requests by the Police can only be actioned under requirements set out in the UK GDPR for authorised Subject Access Requests (see section 8 of this policy). Should a disk/portable device containing footage be required as evidence, a copy may be released to the Police under the procedures described in this policy. Disks/portable devices containing footage will only be released to the Police on the clear understanding that the disk remains the property of TTLT, and both the

disk/portable device and information contained on it are to be treated in accordance with this policy. TTLT also retains the right to refuse permission for the Police to pass to any other person the disk or any part of the information contained thereon. On occasions when a Court requires the release of an original disk this will be produced from the secure evidence disk store, complete in its sealed bag. The Police may require the Academy to retain the stored disks for possible use as evidence in the future. Such disks will be properly indexed and properly and securely stored until they are needed by the Police.

- Applications received from outside bodies (e.g. solicitors) to view or release disks will be referred to the Chief Executive Officer and Data Protection Officer. In these circumstances disks will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.
- Disks are retained for the period in which they are required to fulfil the original purpose of the subject access request. They must then be returned to the Academy for appropriate disposal/deletion/retention in accordance with the TTLT Records Management Policy. The return of the disk/portable device must be logged in the document described in section 6 of this policy.

12. Storage and retention of images

Personal data captured on CCTV footage will be retained and stored in accordance with the principles of the UK GDPR. Footage will be stored on the Academy's system for 31 days, unless retention is required for purposes outlined in this policy; as part of a Subject Access Request or where the Academy is required to submit or retain the data on a legal basis for law enforcement and regulatory purposes.

Recorded material must be stored in a way that maintains the integrity of the information. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used as evidence in court. Academies must consider the medium of storage and the footage must be encrypted; consultation with the DPO should be made to support the maintenance of adequate security measures. Academies must keep a record/audit trail of how the information is handled if it is likely to be used as evidence in court and once there is no reason to retain the recorded information, it should be deleted and the deletion of such data recorded.

Where data is stored, this shall be done so in accordance with the integrity and confidentiality principle of the UK GDPR, on a secure server which is appropriately protected from viruses and unauthorised access, and is located in a secure and lockable location, accessed by authorised personnel only. Authorised personnel includes certified security companies who maintain and support the use of the CCTV system.

Screens and monitoring systems which show the footage must be kept in a lockable room which is inaccessible to unauthorised personnel, and locked/inaccessible to unauthorised personnel when not in use.

Where footage is transferred to portable devices such as disks and USB drives for the purpose of Subject Access Request, these must be encrypted and used in accordance with sections 9 and 10 of this policy. The portable media must be purchased by the Academy and verified by IT Support providers as safe for use (and not subject to cyber security risks such as malware).

Footage must be retained in accordance with the TTLT Records Management Policy.

13. Breaches of the code (including breaches of security)

Any breach of the CCTV Policy and/or the CCTV Code of Practice by TTLT staff will be initially investigated by the Headteacher, in order for them to take the appropriate disciplinary action. The CEO must be informed immediately.

Any breach of the Code of Practice which involves a possible breach of data protection legislation will be reported to the DPO in accordance with the TTLT Data and Cyber-security Breach Prevention and Management Plan, who will support with the reporting of the personal data breach to the ICO within 72 hours of the detection of the breach. TTLT's personal data breach management plan will be consulted and followed.

An independent investigation will be carried out to make recommendations on how to remedy the breach. Findings of the Investigation must be reported to the CEO.

14. Assessment of the Policy

Performance monitoring, including random operating checks, may be carried out by the Data Protection Officer.

15. Complaints and queries

Any complaints about TTLT's CCTV systems should be addressed to the Headteacher of the relevant Academy in the first instance, or in the event of a complaint/concern in relation to personal data, this should be addressed to the Academy's Data Protection Officer as described in the Trust's GDPR Privacy Notice.

Complaints will be investigated in accordance with TTLT's Complaints Policy and Procedures, Data Protection Policy and Records Management Policy.

16. Communication

All staff involved in the operation of CCTV systems will be made aware of this policy and will only be authorised to use the CCTV system in a way that is consistent with the purposes and procedures contained therein.

All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images must ensure that they are compliant with TTLT Data Protection and Records Management Policies.

17. Public information and Freedom of Information Requests

Copies of this policy will be available on the TTLT website.

Academies should have a member of staff who is responsible for responding to freedom of information requests, and understands the Academy's responsibilities. They must respond within 20 working days from receipt of the request. Section 40 of the FOIA and section 38 of the FOISA contain a two-part exemption relating to information about individuals. If academies receive a request for surveillance system information, they are required to consider:

- Is the information personal data of the requester? If so, then that information is exempt from the FOIA and FOISA. Instead this request should be treated as a data protection subject access request as explained above.
- Is the information personal data of other people? If it is, then the information can only be disclosed if this would not breach the data protection principles. In practical terms, if individuals are capable of being identified from the relevant surveillance system, then it is personal information about the individual concerned. It is generally unlikely that this information can be disclosed in response to a freedom of information request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may be unfair processing in contravention of the DPA 2018 and UK GDPR.

When deciding on whether disclosure is appropriate, academies can consider the expectations of the individuals involved, what the information considered for disclosure would reveal and the legitimate public interest in the information. Where you think obscuring images will appropriately anonymise third party personal data, i.e. it is reasonably likely that the requestor or anyone else can identify the individuals whose personal data you wish to protect (disclosure under FOIA being disclosure to the world), then it may be appropriate to do this rather than exempting the information. For example, requestors may ask for information regarding the operation of the systems, the siting of them, or the costs of using and maintaining them. If this information is held, then consideration will need to be given to whether or not it is appropriate to disclose this information under FOIA. If it is not appropriate to disclose this information then an exemption under FOIA will be used, if one is applicable.

Academies who receive a request for CCTV data under the FOIA must consult with the DPO and CEO.

16. Appendices

APPENDIX A REGULATION OF INVESTIGATORY POWERS ACT 2000 PART II APPLICATION FOR AUTHORITY FOR DIRECTED SURVEILLANCE

APPENDIX B REGULATION OF INVESTIGATORY POWERS ACT 2000 RECORD OF REVIEW

APPENDIX C REGULATION OF INVESTIGATORY POWERS ACT 2000 PART II APPLICATION FOR RENEWAL OF DIRECTED SURVEILLANCE AUTHORITY

APPENDIX D REGULATION OF INVESTIGATORY POWERS ACT 2000 PART II - CANCELLATION OF DIRECTED SURVEILLANCE

APPENDIX E REGULATION OF INVESTIGATORY POWERS ACT 2000 CONCLUDING REPORT

APPENDIX A

CONFIDENTIAL WHEN COMPLETE

REGULATION OF INVESTIGATORY POWERS ACT 2000

PART II APPLICATION FOR AUTHORITY FOR DIRECTED SURVEILLANCE

Establishment *(including full address)*			
Name of Applicant		**Position Held**	
Full Address			
Contact Details			
Operation Name (if applicable)			

Details of application:

1. The level of authority required in accordance with the Regulation of Investigatory Powers Act 2000	

CEO	

2. Grounds on which the action is <u>necessary</u>: *delete as inapplicable*
In the interests of national security;
For the purpose of preventing or detecting crime or of preventing disorder;
In the interests of the economic well-being of the United Kingdom;
In the interests of public safety;
For the purpose of protecting public health;
For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

3. Explain why the directed surveillance is proportionate to what it seeks to achieve

4. The identities, where known, of those to be subject of the directed surveillance:	
Name:	

Address:	
DOB:	
Other information as appropriate:	

5. The action to be authorised, including any premises or vehicles involved;
6. Give an account of the investigation or operation;

7. Explanation of the information which it is desired to obtain as a result of the authorisation:

8. Collateral Intrusion:
INDICATE ANY POTENTIAL FOR COLLATERAL INTRUSION ON OTHER PERSONS THAN THOSE TARGETED: INCLUDE A PLAN TO MINIMISE COLLATERAL INTRUSION

9. Confidential/Religious Material:
INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL/RELIGIOUS MATERIAL:

Anticipated Start	**Date:**		**Time:**	

10. Applicant's Details			
Name (print)		**Tel No:**	
Signature		**Date**	

11. Authorising Officer's Comments.

12. Authorising Officer's Recommendation.			
I, [ ], hereby authorise the directed surveillance operation as Detailed above. This written authorisation will cease to have effect at the end of a period of 3 months unless renewed (see separate form for renewals).			
Name (Print)		**POSITION**	
Signature		**Date**	

13. Confidential Material Authorisation.			
Name (Print)		**POSITION**	
Signature		**Date:**	

From Time	**Date:**

14. Urgent Authorisation: Details of why application is urgent.			
Name (Print)		**POSITION**	
Signature		**Date/Time**	

15. Authorising Officers comments. (This must include why the authorising officer or the person entitled to act in their absence considered the case urgent).

16. Please give the reasons why the person entitled to act in urgent cases considered that it was not reasonably practicable for the authorisation to be considered by a person otherwise entitled to act.			
Name (Print)		**POSITION**	
Signature		**Date/Time**	

Appendix B

CONFIDENTIAL WHEN COMPLETE

REGULATION OF INVESTIGATORY POWERS ACT 2000

RECORD OF MONTHLY REVIEW

Public Authority *(including full address)*	

Applicant		**Position Held**	
Operation Name		**Operation Number*** *Filing Ref	
Date Of Authorisation			

2. Detail any significant changes to the information in the original authorisation

3. Explain the continuing need for authority

4. Explain why the directed surveillance is still proportionate to what it seeks to achieve and in particular demonstrate that the degree of intrusion into the privacy of those affected by the surveillance in commensurate with the seriousness of the offence. In particular consideration should be given to:
a) Proportionality *– the use of surveillance must be proportional to the problem it is intended to solve. Levels of intrusion must be appropriate to the severity of the matter under investigation – serious breaches of an individual's right to privacy can only be justified in operations concerning serious crime.* ***(b) Compulsion*** *– is the use of directed surveillance essential to the success of the operation or investigation. It must be demonstrated that other investigative methods either; have been tried without success, are not feasible, not sufficiently reliable or impractical to use in the context of the type of crime or general volume of activity.*

c) Sufficiency of intrusion *– will be directed surveillance be tightly focused on the subject? Is the degree of collateral intrusion affecting individuals not connected with the investigation or operation justifiable and acceptable?*

5. Applicant's Details			
Name (Print)		**Tel No.**	
Position		**Date**	
Signature			

6. Authorising Officers Comments

7. Authorising Officer's Acknowledgment			
Name (Print)		**Position**	
Signature		**Date/Time**	

APPENDIX C

CONFIDENTIAL WHEN COMPLETE

REGULATION OF INVESTIGATORY POWERS ACT 2000

PART II APPLICATION FOR RENEWAL OF DIRECTED SURVEILLANCE AUTHORITY

(Please attach the original authorisation)

Establishment *(including full address)*			
Name of Applicant		**Position Held**	
Full Address			
Contact Details			
Operation Name		**Operation Number*** *Filing Ref	
		Renewal Number	

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	**Date**

2. Detail the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail any significant changes to the information in the previous authorisation.

4. Detail why it is necessary to continue with the authorisation.

5. Indicate the content and value to the investigation of the product so far obtained by the surveillance.

6. Give an estimate of the length of time the authorisation will continue to be necessary.

7. Applicant's Details			
Name (Print)		**Position**	
Signature		**Date/Time**	
8. Authorising Officer's Comments.			

9. Authorising Officer's Recommendation.			
I, [ ], hereby authorise the directed surveillance operation as Detailed above. This written authorisation will cease to have effect at the end of a period of 3 months unless renewed (see separate form for renewals).			
Name (Print)		**POSITION**	
Signature		**Date**	
Renewal From	**Time:**	**Date:**	

APPENDIX D

CONFIDENTIAL WHEN COMPLETE

REGULATION OF INVESTIGATORY POWERS ACT 2000

PART II - CANCELLATION OF DIRECTED SURVEILLANCE

Establishment *(including full address)*			
Name of Applicant		**Position Held**	
Operation Name		**Operation Number*** *Filing Ref	
		Renewal Number	

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

2. Explain the value of surveillance in the operation:

3. Time and Date of when the authorising officer instructed the surveillance to cease.			
Date		**Time**	

4. Authorisation cancelled	**Date:**		**Time:**	

5. Authorising Officer's Recommendation.			
I, [ ], hereby authorise the cancellation of the directed surveillance operation as detailed above			
Name (Print)		**POSITION**	
Signature		**Date**	

APPENDIX E

CONFIDENTIAL WHEN COMPLETE

REGULATION OF INVESTIGATORY POWERS ACT 2000

CONCLUDING REPORT

Establishment *(including full address)*			
Name of Applicant		**Position Held**	
Operation Name		**Operation Number*** *Filing Ref	
Date of Authorisation			

1. Concluding Review – The dates and a brief description of the nature of the surveillance conducted must be recorded in this grid at the conclusion of the authorised surveillance operation			
Date Surveillance undertaken	**Details of any intrusion into privacy of any person involved in or affected by the surveillance**	**Comments/Observations**	**Officer Reporting and date report made**

2. Applicant's Details			
Name (Print)		**Tel No.**	
Position		**Date/Time**	
Signature			
3. Authorising Officer's review observations and recommendations.			

Name (Print)		**Position**	
Signature		**Date**	