

# R5 - Full Data Protection Impact Assessment

## Introduction & Guidance

This form should be completed for any existing/proposed policy/function/project where the initial screening questions indicate a significant impact on our customers/employees/suppliers'/members' personal data.

### Process for completion

- a. The Project Manager/lead officer from the service to complete the DPIA
  - Ensure that you have completed the Initial screening questions and an Information Governance Officer or Data Protection Officer (DPO) had asked you to complete the full DPIA.
  - **Section 1- 6:** Answer concisely but ensure that you have covered the key points
  - **Section 7:** The risk scoring section should be completed with an Information Governance Officer or DPO
  - **Section 8:** Completed by DPO, Information Asset Owner (IAO) and project lead
- b. Send completed DPIA to the Information Governance Officer/DPO who will review and feedback.
- c. Once the review process is completed send to the relevant Information Asset Owner for sign-off.
- d. Hold onto a copy of the signed DPIA with the project documentation and also send a copy to the Information Governance Officer/DPO who will update the RoPA.
- e. All projects (including IT projects) to:
  - capture all identified risks against the GDPR Principles and Data Subjects Rights. Add any agreed mitigations to the risk areas.
  - capture agreed mitigations on the project plan to make sure they are monitored and implemented
  - Projects should not be closed until all agreed mitigations have been implemented or understood and the service area's Information Asset Owner and DPO has confirmed the risks posed by non-implementation of the agreed mitigations are captured on the directorate's risk register.

Please answer all questions/complete all sections.

This is not simply a paper exercise – it is designed to make sure that your policy/function/project and service (development) is delivered fairly to all sections of our local community, and our employees, customers, suppliers and members with their privacy in mind.

Please note that this DPIA may be used to support decisions by members and should form part of papers/reports; therefore, **your completed questionnaire may become a public document, along with other committee papers.** The term 'Proposal' will be used throughout the form as a label for what is being assessed – a new policy, new service, new strategy or a change to an existing policy/service/strategy.

**1. The Proposal being assessed**

<b>Title of proposal being assessed:</b>	Bassetts Park Westfield Road Wellingborough												
<b>What type of proposal is this an assessment of?</b>	New Policy/ Strategy	Policy/ Strategy Change	New Service	Change to Service	Service removal	Project	Other						
<i>Put a x in the correct box</i>						X							
<b>What are the aims and/or objectives of the proposal and the intended outcomes? If assessing the impact of a proposed change please describe the aims of the change, not the original policy/service</b>	<p>North Northamptonshire (Wellingborough) presently has a a CCTV network covering the town centre and areas within the Brickhill and Queensway ward and Hatton Park (Hemmingwell) ward. West Northamptonshire Council monitor and record the Wellingborough network for NNC, which is undertaken at the St John’s Control Room, Northampton.</p> <p>NNCwishes to add another 2 CCTV cameras to the network within Bassetts Park, which is situated in the Croyland and Swanspool ward, to provide safety and security for residents, businesses and facilities users.</p> <p>Bassetts Park is a central Park close to town centre which has play facilities for toddler and junior children, a bandstand and a skatepark within the grounds.</p> <p>The park has experienced anti-social behaviour, especially around the old skatepark where people sit under ramps; the area has no lighting so in the dark cannot be seen as it is located at the back of the park with no natural surveillance.</p> <p>A new skatepark is proposed in a better visible location of the park, subject to planning consent. To help address the concerns of residents/police around ASB/crime,a recommendation from the Police is that consideration is given to providing CCTV in the park..</p> <p>Wellingborough has disproportionate higher levels of crime in comparison to other medium sized towns in England &amp; Wales. In 2020 Wellingborough’s crime statistics were 32% higher than Northamptonshire as a whole. Outlined below shows the recent crime statics in Wellingborough over the past 12 months.</p> <p>Other solutions have been considered and are included within the application more lighting so the skatepark would be seen at night and is safe for skaters to use in the dark, the location is more visible by passer bys aswell as park users. Near other facilities of the park so all ages can use without feeling intimidated.</p> <table border="1" data-bbox="435 1835 1442 1873"> <tr> <td>Location</td> <td>Camera</td> <td>Amount</td> <td>Recording</td> <td>Monitoring</td> <td>Assessment</td> </tr> </table>							Location	Camera	Amount	Recording	Monitoring	Assessment
Location	Camera	Amount	Recording	Monitoring	Assessment								

	Type	types used				of use of equipment (mitigations or justifications)
	Bassetts Park	Standard PTZ/HD PTZ	2	24hrs	24hrs. Max 1 Operators High level	
<b>Who is intended to benefit from this proposal?</b>	Residents, skaters and park users of Bassetts Park					
<b>Who are the main stakeholders in relation to the proposed proposal?</b>	These are the Council, Elected Members, residents, Police.					
<b>Consultation required? Describe how &amp; when you will seek individuals' or stakeholders' views – or justify why it is not appropriate to do so</b>	Many residents objected to the proposals in the previous planning application. The Police have given a strong recommendation that CCTV should be considered if there is to be a skatepark build within the park so it would help deter and ASB/crime from users of the skatepark and for the safety of the park users to reduce the fear of crime.					
<b>Service Area/Team with responsibility for implementation of this proposal</b>	Rajvinder Gill – Capital projects team (development of the Skatepark project) Mike Greenway, Strategic Lead, - Safer Communities Team, North Northamptonshire Council. (CCTV management)					
<b>Name and job title / role of person completing full Screening:</b>	Kish Lad, Community Services Officer, Safer Communities Team -(Kettering) North Northamptonshire Council.					
<b>Date completed:</b>						

## 2. Privacy Impact – what are we collecting and how?

2.1	<b>Is this a new type/s of personal information <u>or</u> information that is already collected?</b>	New	<u>Existing</u>
2.2	<b>What data will be collected?</b>  Images will be collected 24/7 and stored for 31 days after which they are deleted. There will be processing of data in response to situations real time following Police requests, from North Northamptonshire Council (Wellingborough) managers, operatives responding to situations		

	<p>developing in front of them, system checks and following requests to review as set out in the policy and procedures.</p> <p>Images will be collected of members of the public going about their daily business in the park. There may be times that children and vulnerable groups have images collected of them but these will only be processed should the need arise to safeguard or protect them.</p>		
	<b>Administration data</b>		<b>Sensitive data</b>
	Forename		Racial or ethnic origin ✓
	Surname		Political opinion
	Date of Birth		Religious belief
	Age		Trade Union membership
	Gender	✓	Health or Social Care Status
	Address		Sexual life and/or Sexual orientation
	Postcode		Commission or alleged commission of an offence
	Unique Identifier (i.e. NI number or similar)		Proceedings for any offence committed or alleged ✓
	Other data ( <i>Please state</i> )		
	N/A		
	Will the dataset include health/social care data?		No
	Will the dataset include financial data?		No
	Detailed description of other data collected: ( <i>If there is any additional feature of the dataset that we should be made aware of, please state it here</i> ).		
	N/A		
2.3	<b>How will we collect the data?</b>		
	<p>1. Live video images collected real-time by CCTV cameras.</p> <p>2. Live video images stored securely, no integrated surveillance technologies will be used.</p> <p>3. All live video recordings will be stored, but not accessed or reviewed until necessary or requested. this will be undertaken by trained and qualified staff.</p> <p>4. All CCTV footage to be deleted after 31 days in line with guidelines on a rolling basis.</p>		
	<b>Please state by which method the information will be collected?</b>		
	Visual electronic data only		

	Email <i>(Please state whether it is via secure mail (gcsx.gov) or non-secure .gov mail)</i>	
	Face to face	
	Courier	
	Web form	
	Post (internal)	
	Post (external)	
	By Hand	
	Telephone	
	Referral form/other external agency	
	Other (please specify)	✓
	<ul style="list-style-type: none"> <li>• Fixed CCTV (networked)</li> <li>• Body Worn Video</li> </ul>	
2.4	<b>Will the information be collected electronically, on paper or both?</b>	Electronically – The local authority CCTV Control room. The system’s technology enable recording.
2.5	<b>How will individuals be informed about the proposed uses of their personal data?</b>	<p>Public Space CCTV cameras are all signed clearly displaying information on who the system owner is and how to make contact. Other internal areas where there are surveillance camera systems display signage around the facility and car park, making all visitors and staff aware the system is live and in place. The councils privacy policy is available on the website which is promoted to all. The council has a robust process in place for dealing with GDPR requests, which will be used. Customers and staff are made aware of the system and why this is required, for the safety and security of all.</p> <p>The <u>Closed circuit television (CCTV) and surveillance privacy noticeprivacy policy is available on the NNC website.</u></p>
<b>3. Privacy Impact – how do we use/process/store the data?</b>		

3.1	<p><b>Describe in as much detail <u>why</u> this information is being collected/used</b> – explain the nature of the relationship with the individuals, how much control do they have, would they expect you to use their data in this way. Does the processing include children’s data or vulnerable groups?</p> <p>North Northamptonshire Council (Wellingborough) has installed CCTV (Closed Circuit Television) cameras in various locations within the conurbation for the purposes of reducing crime, disorder, anti-social behaviour and the fear of crime by helping to provide a safer environment for those people who live and work in the area and for visitors travelling through the area. CCTV is also installed on highways for monitoring traffic on a permanent or temporary basis. In all locations, signs are displayed notifying you that CCTV is in operation and providing details of who to contact for further information about the scheme. The purpose and use of the CCTV system are to provide the Police and enforcement agencies with assistance to detect, deter and prevent crime and disorder; to help identify, apprehend and prosecute offenders; to provide the Police/Council with evidence to enable criminal and/or civil proceedings to be brought in the courts; and to maintain public order.</p> <p>Some examples of how data is used is provided below:</p> <ul style="list-style-type: none"> <li>• Providing evidence in criminal proceedings (police and criminal evidence act 1984 and criminal procedure and investigation act 1996)</li> <li>• Providing evidence in civil proceedings</li> <li>• The prevention and reduction of crime and disorder</li> <li>• The investigation and detection of crime</li> <li>• Identification of witnesses</li> </ul> <p>Effectiveness of the system is measured regularly along with information supplied by the police and other council departments. Effectiveness of the system along with compliance with the Protection of Freedoms Act 2012 and SC Code of Practice, GDPR/DPA is measured through SCC Certification process.</p> <p>The information is used to:</p> <ul style="list-style-type: none"> <li>• Monitor in real time to detect and respond to unlawful activities; track suspicious persons / activity.</li> <li>• Used to search for vulnerable persons and wanted persons.</li> <li>• Recorded data is discussed to authorised agencies to support post incident investigation, including law enforcement agencies.</li> <li>• Recorded data is disclosed to authorised agencies to provide intelligence.</li> </ul>
3.2	<p><b>Please complete this section if you are not relying on consent as a legal basis for</b></p> <p style="text-align: center;"><u>Personal Data</u> (Article 6)</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Contract</li> <li><input checked="" type="checkbox"/> Legal obligation</li> <li><input checked="" type="checkbox"/> Vital interests</li> <li><input checked="" type="checkbox"/> Public task</li> </ul>

	<p><b>processing this information</b></p>	<p><input type="checkbox"/> Legitimate interests (Non-public tasks only, e.g. HR)</p> <p style="text-align: center;"><b><u>If processing Special Category Data (Article 9)</u></b></p> <p><input type="checkbox"/> (a) Explicit consent</p> <p><input type="checkbox"/> (b) Employment, social security and social protection (if authorised by law)</p> <p><input checked="" type="checkbox"/> (c) Vital interests</p> <p><input type="checkbox"/> (d) Not-for-profit bodies</p> <p><input checked="" type="checkbox"/> (e) Made public by the data subject</p> <p><input checked="" type="checkbox"/> (f) Legal claims or judicial acts</p> <p><input checked="" type="checkbox"/> (g) Reasons of substantial public interest (with a basis in law)</p> <p><input type="checkbox"/> (h) Health or social care (with a basis in law)</p> <p><input type="checkbox"/> (i) Public health (with a basis in law)</p> <p><input type="checkbox"/> (j) Archiving, research and statistics (with a basis in law)</p> <p style="text-align: center;"><b><u>If processing Criminal Data (Article 10)</u></b></p> <p><input checked="" type="checkbox"/></p> <p><b><u>Data Protection Act Schedule 1</u></b></p> <p><input checked="" type="checkbox"/> Part 1 Part 1 (3) (2) (b) (ii)</p> <p><input type="checkbox"/> Part 2</p> <p><input type="checkbox"/> Part 3</p> <p><b><u>Principal Legislation</u></b></p> <p>The lawful basis is that North Northamptonshire Council are undertaking CCTV processing to perform a task carried out in the public interest and in exercising our official duty under the Crime &amp; Disorder Act 1998 Section 17; Police and criminal evidence act 1984 and criminal procedure and investigation act 1996).</p> <p>to deter and prevent crime and disorder. There will also be at times processing necessary in order to protect the vital interests of the data subject for matters of life or death.</p>
3.3	<b>Where will the</b>	Fixed CCTV (networked) - Live video images stored securely; no integrated surveillance technologies will be used. All live video recordings will be stored,

	<p><b>information be stored?</b> (What system is the data stored on)</p>	<p>but not accessed or reviewed until necessary or requested. This will be undertaken by trained and qualified staff.</p> <p>Body Worn Video – Live images and sound stored on secure encrypted units. Every week the units are taken to the Local Authority control room where any images needed are downloaded to file and the remaining are deleted.</p> <p>The data will be stored on a hard drive, with the technology to automatically override the video footage when out of the 31-day period. The system is stand-alone but will meet all the council's necessary ICT safeguarding restrictions to ensure it complies. The hardware and system access will only be accessible by trained and authorised staff. The disclosure of images is controlled and in accordance with the CCTV Code of Practice.</p>
3.4	<p><b>Is there an ability to audit access to the information?</b></p>	Yes
3.5	<p><b>Does the system/solution involve new links with personal data held in other systems or have existing links been significantly changed?</b></p>	No
3.6	<p><b>Will the information be kept up to date and checked for accuracy and completeness (data quality)?</b></p> <p>Effectiveness of the system is measured regularly along with information supplied by the police and other council departments. Effectiveness of the system along with compliance with the Protection of Freedoms Act 2012 and SC Code of Practice, GDPR/DPA is measured through SCC Certification process.</p> <p>The system is subject to regular audits and security tested regularly.</p>	Yes
3.7	<p><b>Who will have access to the information?</b> <i>Consider whether access will be granted to temporary or contract staff – how will this be managed?</i></p>	<p>NNC is the system owner. CCTV Operatives will be managing the system on a daily basis. and they have all completed training on GDPR, Safeguarding, RIPA and Human Rights and are PSS SIA licensed. The CCTV maintenance company would also be required to access the system as part of their maintenance works.</p> <p>Footage will be stored on site in a secure and restricted access room. Access will only be available to trained staff with designated authority to do so.</p> <p>Recording is enabled and this is undertaken at the Local Authority CCTV Control room.</p> <p>North Northants Unitary are the system owners. CCTV Operatives will be managing the system on a daily basis and they have all completed training on GDPR, Safeguarding, RIPA and Human Rights and are PSS SIA licensed.</p>



	<p>The CCTV maintenance company would also be required to access the system as part of their maintenance works.</p> <p>The Surveillance Code of Practice includes details in relation to data sharing agreements and when data can and cant be shared. The lawful basis for processing is to enable us to carry out our public task functions as set out in the Crime &amp; Disorder Act 1998.</p> <p>There are written policies specifying the agencies that are granted access and how infirmation is disclosed. These procedures are made public.</p> <p>There are auditing mechanisms. Any operation to do with CCTV is audited. This includes the use of cameras, reviewing and downloading images, access, storage and incidents recorded.Regular audits are carried out by the CCTV manager. Annual assessment in compliance with the SCC Certification and a council audit every three years.</p>	
3.8	<b>What security and audit measures have been implemented to secure access to and limit use of personal identifiable information?</b>	
	Username and password	✓
	Swipe/Access card	
	Key to locked filing cabinet/room	
	Multi-factor authentication/ Remote Access process (state how many – if none put 0)	
	Restricted access to Network Files	✓
	Other ( <i>Provide a description below</i> )	
3.9	<b>Are there any new or additional reporting requirements for this project?</b>	No
	Who will be able to run reports?	
	Who will receive the report or where will it be published?	
	Report format:	
	Personally identifiable format?	No
	Pseudonymised format? De-identify data this means the data is no longer attributed to a specific subject only with additional information	Yes
	Anonymised format? Data is not or no longer identifiable	Yes

#### 4. Privacy Impact – how do we share personal data?

4.1	<p><b>Are other organisations involved in processing / using the data?</b> <i>(If yes please list)</i></p> <p>Copies of footage released is shared with Northants Police.</p> <p>Copies may be released to law enforcement agencies, insurance companies and solicitors who request footage under Schedule 2 Data Protection Act 5 (3). Sometimes this is hand delivered. The footage will be downloaded onto either encrypted USB or CD and sent by Recorded delivery. On receipt of the USB / CD, the encryption code will be passed to the requester. Access is restricted to the control room and system.</p> <p>The Surveillance Code of Practice includes details in relation to data sharing agreements and when data can and can't be shared.</p> <p>There is a LANDesk system in place where electronic requests are received. Footage is collated in evidence bags and then collected on a weekly basis by courier. For urgent requests the Officer will attend in person - both methods require documentation and signing over to accept responsibilities as the data controller.</p> <p>For other reasons encrypted discs are delivered via recorded post to insurance companies or hand delivered and signed for on proof of identity if in the borough through the SAR process. Records are completed of any information disclosed for audit and compliance purpose.</p> <p>The shared data is used to:</p> <ul style="list-style-type: none"> <li>• Monitor in real time to detect and respond to unlawful activities; and to track suspicious persons/activity.</li> <li>• Search for vulnerable and wanted persons.</li> <li>• Provide intelligence to authorised agencies.</li> </ul>	Yes
4.2	<p><b>Will external contractors have access to the personal data.</b> <i>(E.g., independent investigators, management consultants) (If yes please give details)</i></p> <p>Contracted maintenance operatives will have access to the system for improvement and fault rectification works. The contract details confidentiality and the associated legislation and compliance, and the ramifications if breached.</p>	Yes
4.3	<p><b>Will any information be sent offsite – i.e., outside of the organisation and its computer network (including cloud computing)</b> <i>(If yes please give details)</i></p>	Yes

	<p><i>below including whether you are transferring personal data to a country or territory outside of the UK, or where suppliers' servers are based).</i></p> <p>Data is downloaded (encrypted) onto discs and memory sticks (encrypted) and then persons sign to acknowledge they are now the Joint Data Controllers and accept responsibility. In relation to SARs (subject access requests) proof of id is required prior to handing over. Insurance claims are sent recorded delivery. All transfers are undertaken in this country.</p>	
4.4	<p><b>Is there an information sharing agreement or contract in place for the above activity?</b> <i>(If yes, please provide the location of the agreement and the review date/responsible officer.)</i></p> <p>There is an ISA with Northants Police in relation to releasing footage for investigation purposes.</p>	Yes
4.5	<p><b>Please state by which method(s) the information is/will be transferred?</b> <i>Tick each one that applies</i></p>	
	Secure Email (if so what type)	
	Secure File Transfer Protocol (SFTP)	
	Encrypted removable media device (USB)	✓
	Secure Cloud Storage Transfer	
	Courier	✓
	Secure Website access	
	Post (internal)	
	Post (external)	
	By Hand	✓
	Telephone	
	Wireless network	
	Other (please specify) <ul style="list-style-type: none"> <li>Encrypted disks</li> </ul>	
4.6	<p><b>Do we have active consent notices in place for customers/employees to consent for their information to be collected/processed and/or shared?</b></p>	Yes – Privacy notices in place.
<p><b>5. Privacy Impact – how and when do we archive/dispose of the data collected?</b></p>		

5.1	<p><b>If/when this new/revised function concludes, are there plans in place for how the information will be retained / archived/ transferred or disposed of?</b> <i>(If yes, please give details below)</i></p> <ul style="list-style-type: none"> <li>Fixed CCTV (networked) – All CCTV footage is automatically deleted after 31 days in line with guidelines on a rolling basis, unless footage has been requested, this would be recorded and passed forward to the relevant organisation for evidence purposes for prosecution. Footage could be stored in the evidence locker to give investigating authorities and data subjects sufficient time to request footage.</li> <li>Body Worn Video – All activity recorded in the daily log by the CCTV Operative and all processing undertaken by them.</li> </ul>	Yes
5.2	<p><b>If this information is held in paper records, are they destroyed securely?</b></p>	Yes
<b>6. Privacy Impact – how do we ensure the correct process is followed?</b>		
6.1	<p><b>Is Mandatory Employee Training in place for the following?</b></p> <p>Data Collection (i.e. the process)</p> <p>Use of the System or Service</p> <p>Collecting Consent</p> <p>Data Protection:</p>	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p>
6.2	<p><b>Are arrangements in place for recognising and responding to requests for access individuals' personal data?</b></p> <p>NNCs CCTV policies and procedures are fully compliant with the UK GDPR and DPA 2018 for general disclosure access requests and CCTV related subject access requests.</p> <p>The council has a robust process in place for dealing with individual rights requests under UK GDPR. Details of how to action these are included in the CCTV privacy notice. Further Information on subject access can be found on the NCC website.</p> <p>All requests are initially dealt with by the Information Governance Department – Data Requests Team. These are then passed to the CCTV Manager.</p> <p>Customers and staff are made aware of the system and why this is required, for the safety and security of all.</p> <p>Any complaints are dealt with through the councils complaints procedures.</p>	Yes

*Now contact your Information Governance Officer or Data Protection Officer and work with them to complete the risk scoring and action planning form below, which will detail the changes that need to be made to this service/policy/function to optimise compliance with our data protection duties*

# DPIA – Risk Assessment Scoring – Section 7

**This section will be filled-in in conjunction with your Information Governance Officer or DPO.** This section is a culmination of the answers you've provided in the rest of the DPIA. The misuse of personal data could lead to significant impacts on Individuals/data subjects such as our service users, residents, staff etc. – This could be that they cannot exercise their rights or there has been a data breach. The council could also be fined if the processing doesn't comply with data protection legislation.

- A **risk** is something that may occur
- An **issue** is something that has occurred
- In calculating risk, there are two components ( $Risk = Likelihood * Impact$ ):
- the **likelihood** of a risk materialising to become an issue
- the **impact** that will be felt if the risk occurs.
- A **mitigation** is a control, measure, action we can take to either stop/reduce the likelihood of the risk occurring or reduce the impact if the risk does occur (i.e. if the risk becomes an issue).

Below, there are descriptions for scoring the respective Likelihood (probability) and Impact ratings – Use these tables to give a rating to the likelihood and impact elements of each risk you identify. We will assess the risk of not complying with the Data Protection Principles and the Rights. Any potential issue can be aligned to a Principle

Description of likelihood		Description of impact ratings		
Likelihood	Description	Impact Level	Reputation	Legal / Regulatory
5. Almost certain	Almost certain to occur 81% to 100% chance of occurrence	5. Catastrophic	Critical impact on business reputation and/or national media exposure.	Regulatory and high level Government intervention/action.
4. Likely	More likely to occur than not 51% to 80% chance of occurrence	4. Major	Significant impact on business reputation and/or national media exposure.	Management challenged / Large legal liabilities. Likely to result in regulatory intervention/action.
3. Possible	Likely to occur 21 to 50% chance of occurrence	3. Moderate	Moderate to small impact on business reputation.	Management reviewed / legal reserves established. Triggers regulatory investigation.
2. Unlikely	Very unlikely to occur 6 to 20% chance of occurrence	2. Minor	Some impact on business reputation.	Minimal / limited liabilities. Requires immediate regulator notification.
1. Rare	Virtually impossible to occur 0 to 5% chance of occurrence.	1. Insignificant	No impact on business reputation.	Minimal liabilities. No immediate regulator notification required.

# DPIA – Risk Assessment Scoring – Section 7

Inherent Risk				Issue and Mitigation	Residual Risk		
Privacy Risks	Likelihood (L)	Impact (I)	Risk rating (L x I)		Likelihood (L)	Impact (I)	Risk rating (L x I)
<p><b>Lawfulness, Fairness, And Transparency</b></p> <ul style="list-style-type: none"> <li>The data subjects (service users, customers, staff) <b>have not been notified of or consented to</b> their personal and special categories/criminal offence data being processed for the purposes of this project/procurement/initiative. If notification rather than consent, the legal basis for processing must be stated.</li> <li><b>We don't have a legal basis</b> (lawful basis for processing personal data and additional conditions for processing special categories and criminal offences data) for our proposed processing.</li> </ul>	N/A	N/A	N/A	Lawful basis is established in section 3.2.	N/A	N/A	N/A
<p><b>Purpose Limitation</b></p> <ul style="list-style-type: none"> <li>The personal and special categories/criminal offence data sets to be handled <b>aren't collected for specified, explicit, and legitimate purposes.</b></li> <li>The personal and sensitive data sets to be handled will <b>be processed in a manner that is incompatible with those purposes.</b></li> </ul>	N/A	N/A	N/A	<p>N/A information is collected for legitimate purposes as defined in s3.2.</p> <p>No cameras will look into properties these will be only facing monitoring the park</p>	N/A	N/A	N/A
<p><b>Data Minimisation</b></p> <ul style="list-style-type: none"> <li>The personal and special categories/criminal offence data to be handled are <b>not adequate, relevant and limited</b> for the purposes of task in hand.</li> </ul>	1	1	1	<p>The minimum amount of data is collected. The categories of personal and special category data have not changed. Recording is set on a tour to pan around unless overridden in response to a situation and only reviewed if requested</p>	1	1	1

# DPIA – Risk Assessment Scoring – Section 7

				and in line with criteria as set out in the Code of Practice.			
<p><b>Accuracy</b></p> <ul style="list-style-type: none"> <li>The personal and special categories/criminal offence data to be handled contains <b>inaccuracies</b> that will skew the accuracy of decisions taken.</li> </ul>	N/A	N/A	N/A	Live recorded images can't be amended, if data was deliberately deleted there would be an audit trail of users.	N/A	N/A	N/A
<p><b>Storage Limitation</b></p> <ul style="list-style-type: none"> <li>The personal and special categories/criminal offence data handled is <b>retained</b> for longer than is necessary for the purposes for which it is processed.</li> </ul>				<p>The recorded data of the CCTV footage is stored for up to 31 days, then automatically deleted. Unless footage has been requested, this would be recorded and passed forward to the relevant organisation for evidence purposes for prosecution; or stored in the evidence locker. This should give investigating authorities and Data Subjects sufficient time to request footage.</p> <p>Under certain circumstances authorised persons may override the retention period, e.g. retained for prosecution agency.</p> <p>Measures are in place (SIA licensed staff, regular training, Supervisor undertaking audits to monitor access to files). Security at camera locations has been reviewed and upgraded. Footage will be stored on site in a secure and restricted access room. Access will only be available to trained staff with designated authority to do so. Static camera covers the control room with only the Supervisor having access to view it retrospectively.</p>	N/A	N/A	N/A



# DPIA – Risk Assessment Scoring – Section 7

				<p>Under s4.5 the method of transfer is via courier/post and on an encrypted removeable media device (USB). Secure File Transfer Protocol (SFTP) would be the preferred method to protect the data in transit, which is paramount. If this was implemented this would prevent the data being lost/stolen/unlawfully accessed.</p> <p>Risk:</p> <p>Unauthorised Disclosure may result in prosecution under GDPR/DPA 2018 and subject to financial penalties and severe damage to the reputation of the local authority.</p> <p>Mitigation:</p> <p>Release of data is strictly controlled by the council. Information Sharing Agreement in place with Police. All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. CCTV staff trained in unauthorised disclosure and misuse of data.</p> <p>Risk:</p> <p>Security of Data. A Security Data breach may result in prosecution under GDPR/DPA 2018 and result in financial penalties and severe damage to the reputation of the local authority</p> <p>Mitigation:</p>			
--	--	--	--	--	--	--	--

# DPIA – Risk Assessment Scoring – Section 7

				<p>Security of Data Management of the use and security of the system including monitoring, reviewing and downloading of footage. Regular audits carried out and SCC Certification achieved. Spot checks on proactive monitoring by staff, use of passwords and checks carried out by maintenance contractors for network security.</p> <p>Risk:</p> <p>Misuse of data may result in prosecution under GDPR/DPA 2018 and subject to financial penalties and severe damage to the reputation of the local authority.</p> <p>Mitigation:</p> <p>Release and use of data are strictly controlled by the council. All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. CCTV staff trained in unauthorised disclosure and misuse of data.</p>			
<p><b>Integrity and Confidentiality (Security)</b></p> <ul style="list-style-type: none"> <li>Personal and special categories/criminal offence data is processed in a manner that is not secure – there is not an appropriate level of technical and organisation measures taken to protect the data against <b>unauthorised</b> or <b>unlawful</b> processing and against <b>accidental loss, destruction</b> or <b>damage</b>.</li> </ul>	3	3	9	<p>Copies may be released to law enforcement agencies, insurance companies and solicitors who request footage under Schedule 2 Data Protection Act 5 (3). (sometimes it is hand delivered). The footage will be downloaded onto either encrypted USB or CD and sent by Recorded delivery. On receipt of the USB/CD, the encryption code will be passed to the requester. Access is restricted to the</p>	1	1	1

# DPIA – Risk Assessment Scoring – Section 7

				<p>control room and system. The system has multi-layer password protected and use is subject to regular audits. The system is security tested regularly.</p> <p>No international transfers are made.</p> <p>Management of the use and security of the system including monitoring, reviewing and downloading of footage. Regular audits carried out and SCC Certification achieved. Spot checks on proactive monitoring by staff, use of passwords and checks carried out by maintenance contractors for network security.</p> <p>Release and use of data are strictly controlled by the council. Information Sharing Agreement in place with Police. All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. CCTV staff trained in unauthorised disclosure and misuse of data.</p> <p>All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. CCTV staff trained in unauthorised disclosure and misuse of data.</p>			
<p><b>Accountability</b></p> <ul style="list-style-type: none"> <li>We are unable to demonstrate compliance with the data protection principles for the</li> </ul>				<p>Compliance with GDPR/DPA, POFA, Code of Practice and operating procedures reduces the risk of</p>			

# DPIA – Risk Assessment Scoring – Section 7

<p>processing of the personal and special categories/criminal offence data:</p> <ul style="list-style-type: none"> <li>a. Lawful, fair and transparent</li> <li>b. Purpose limitation</li> <li>c. Data minimisation</li> <li>d. Accuracy</li> <li>e. Storage limitation</li> <li>f. Security</li> </ul>				<p>unauthorised disclosure or the misuse of data. SCC Full certification achieved, and regular audits are carried out by the system manager.</p> <p>Compliance with GDPR/DPA 2018. Management of the use and security of the system including monitoring, reviewing, and downloading of footage. Regular audits carried out and SCC Certification achieved.</p> <p>Compliance with articles 4, 6 and 13 of the Human Rights Act Management of the use and security of the system including monitoring, reviewing, and downloading of footage. Regular audits carried out and SCC Certification achieved. Spot checks on proactive monitoring by staff.</p> <p>Compliance with SC Code of Practice and the Protection of Freedoms Act Management of system. SCC Full certification.</p>			
<p><b>International Transfers</b></p> <ul style="list-style-type: none"> <li>• Personal and special categories/criminal offence data is processed outside of the UK without appropriate safeguards in place.</li> </ul>	N/A	N/A	N/A	There are no international transfers.	N/A	N/A	N/A
<p><b>Data Subject Rights</b></p> <ul style="list-style-type: none"> <li>• The processing of personal and special categories/criminal offence data is processed in a manner that does not comply with the rights of data subjects:             <ol style="list-style-type: none"> <li>1. the right to be <b>informed</b></li> <li>2. the right of <b>access</b></li> </ol> </li> </ul>	N/A	N/A	N/A	The NNC `s CCTV policies and procedures are fully compliant with the GDPR/DPA 2018 for general disclosure access requests and CCTV related subject access requests. Information on subject access can be found on the NCC council website and all requests are initially dealt	N/A	N/A	N/A

# DPIA – Risk Assessment Scoring – Section 7

<p>3. the right to <b>rectification</b>          4. the right to <b>erasure</b>          5. the right to <b>restrict processing</b>          6. the right to data portability          7. the right to object          8. Rights <b>related to data portability</b></p>				<p>with by the Data Protection Governance Team and then passed to the CCTV Manager.</p> <p>Any complaints are dealt with through the council's complaints procedures.</p> <p>Compliance with SC Code of Practice and the Protection of Freedoms Act 2012.</p>			
<p><b>Overall Risk Exposure Score (Average)</b></p> <p><i>Add the score in the Likelihood column and divide by 9</i></p> <p><i>Add the score in the Impact column and divide by 9</i></p>	1.1	0.9	1		0.7	0.7	0.5

Risk level - State the number of risks in each category	Initial Score	Residual Score
<b>Low 1-10 - Project can proceed</b>	<b>1</b>	<b>0.5</b>

## 8. Sign off and Record Outcomes

Item	Name/date	Notes
Measures approved by:	Mike Greenway Strategic Lead for Community Safety 17.01.2024	
Residual risks approved by:	Mike Greenway Strategic Lead for Community Safety 17.01.2024	
DPO advice provided:	Naomi Harewood 30.11.2022	

Summary of DPO advice:

Privacy Notices:

- Ensure the DSA with the police is up to date and fit for purpose. Please review as necessary.

Accountability:

- Ensure this processing is included in the Service Area Record of Processing Activities (ROPA) or in the service areas Information Asset Register.
- Ensure that any agency staff are trained to the same standard as permanent / fixed term staff.

Integrity and Confidentiality (Security):

- Use organisational measures and run regular reports to assess who is accessing the footage.
- Under s4.5 the method of transfer is via courier / post and on an encrypted removeable media device (USB). Secure File Transfer Protocol (SFTP) would be the preferred method to protect the data in transit, which is paramount. If this was implemented this would prevent the data being lost/stolen/unlawfully accessed. [The Greater Manchester Police has been fined £150,000 after three DVDs containing footage of interviews with victims got lost in the post.](#) Consider the use of SFTP. Kettering ICT have access to this facility.

Accepted risks should be recorded on the service areas risk register.

DPO advice accepted or overruled by:	Mike Greenway Strategic Lead for Community Safety 17.01.2024	If overruled, you must explain your reasons
Comments:  Accepted / <del>Overruled</del>		
Consultation responses reviewed by:	Mike Greenway Strategic Lead for Community Safety 17.01.2024	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:	Information Governance Department	The DPO should also review ongoing compliance with DPIA

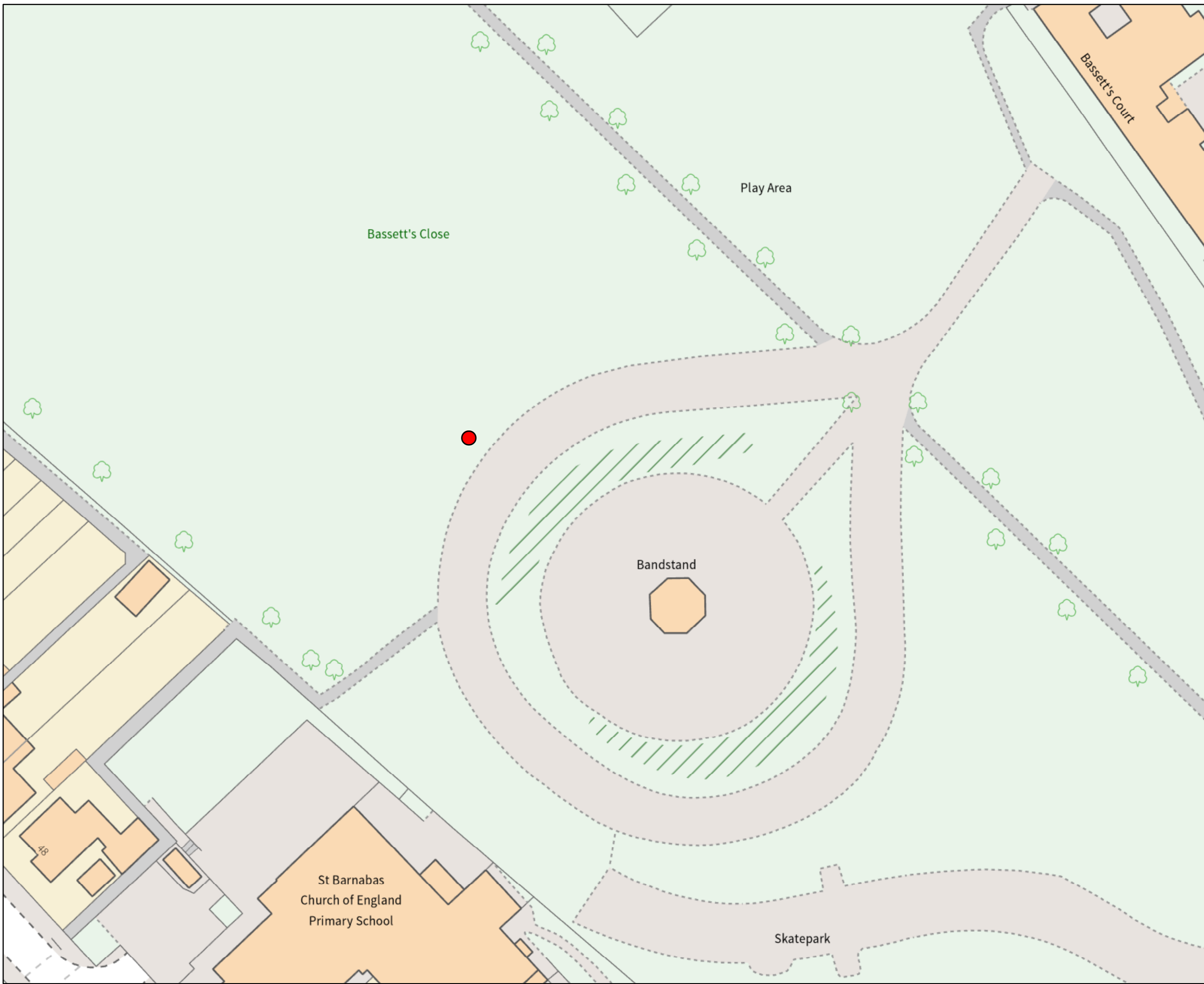
This completed document should be shared with your line manager and with the Data Protection Officer. Refer to the completion of the DPIA in the Human Rights Implications' section of your report and to ask for the DPIA to be taken into consideration when a decision is being made.



Scale:  
1:500

Wellingborough

new CCTV camera  
Bassett's Close



This map is accurate to  
the scale specified above  
when reproduced at:  
A3





Scale:  
1:500

Wellingborough

new CCTV camera  
West Villa Road

This map is accurate to the scale specified above when reproduced at:  
A3

© Crown Copyright and database right 2023.  
Ordnance Survey AC0000843726

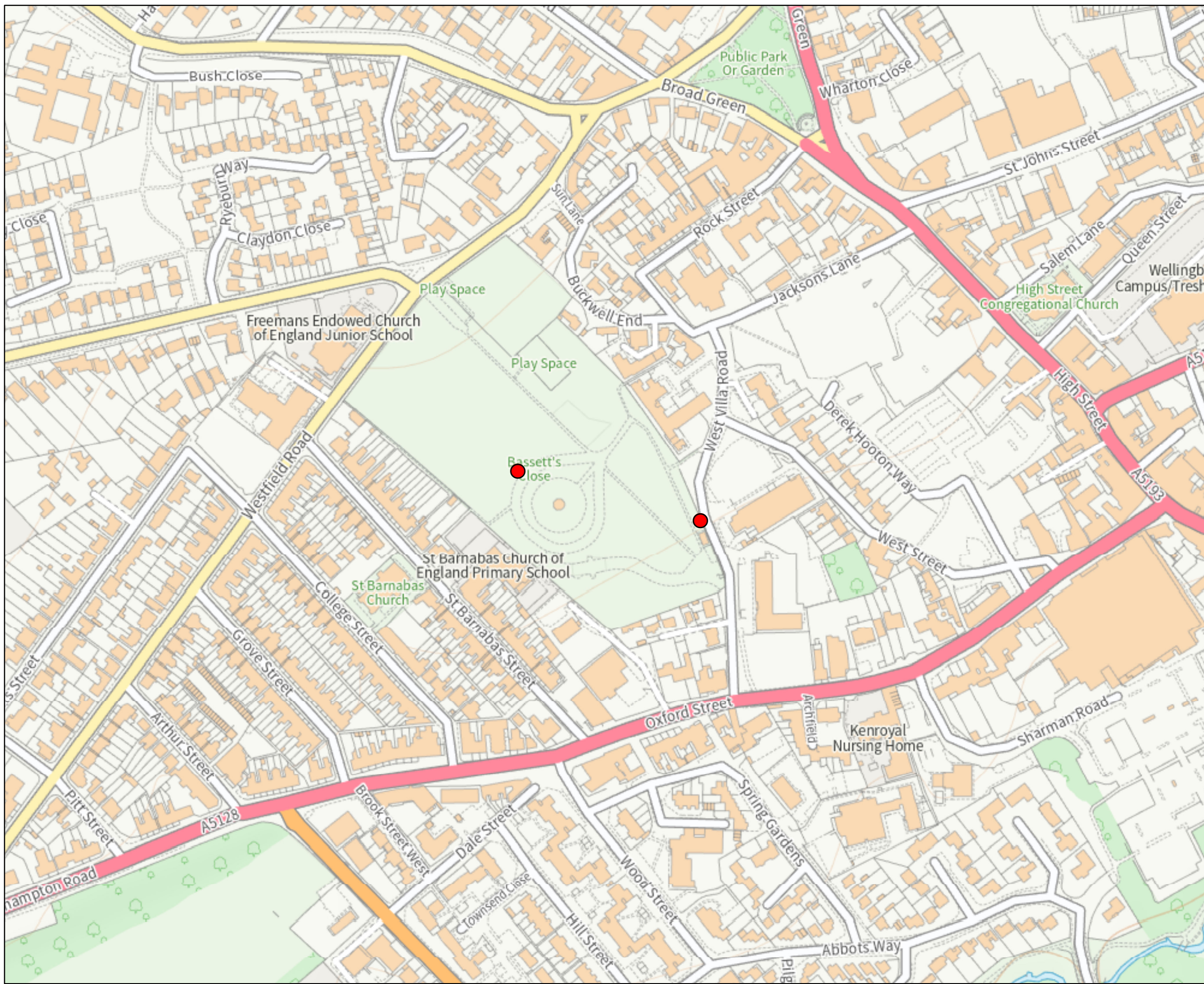




Scale:  
1:2,500

Wellingborough

2x new CCTV cameras location map



This map is accurate to the scale specified above when reproduced at: A3



Installation of new CCTV cameras and associated equipment in .....

**CCTV Camera technical specification**

- The CCTV cameras provided as part of the contract to install the CCTV will meet the following technical specification:

Component	Item	Specification	
General	Dimensions	Ø 240mm to 266.6mm Height: maximum of 410mm	
	Weight	Maximum 8 kg.	
	Function	Mirror, password protection, watermark, IP address filter	
	Operating environment		Outdoor temperature: -40° to +70° Celsius
			Humidity: ≤ 90%
	Language	English required. Multiple language capability accepted.	
	Power	24 VAC (max. 60W including max.18W for IR and max.6W for heater. Hi-PoE (max. 50W including max.18W for IR and max.6W for heater)	
	Resistant to	Dust particles, precipitation from weather and sunlight.	
Wiper	Required		
DORI calculation	Standard	BS EN 62676 part 4: 2015	
	Detect	Definition: 25px/m – Distance: 2034.5m	
	Observe	Definition: 63px/m – Distance: 807.3m	
	Recognise	Definition: 125px/m – Distance: 406.9m	
	Identify	Definition: 250px/m – Distance: 203.4m	
Audio capability	Compression/ (bit rate)	G.711/(64Kbps)	
Camera	Image sensor	1/1.8" progressive scan CMOS	
	Illumination	Colour: 0.002 LUX (F1.5, AGC ON)	
		Black and white: 0.0002 LUX (F1.5, AGC ON)	

		With IR – 0 LUX
	Shutter speed	1/1 s to 1/30,000 s
	Zoom	Optical: 25x ; Digital: 16x
	Day and night vision	IR cut filter
	Resolution	Maximum: 1920 x 1080
Camera Lens	Aperture	Maximum F1.5
	Field of View	Horizontal: 59.8° to 3.3° (wide-tele) Vertical: 33.7° to 1.9° (wide-tele) Diagonal: 65° to 3.8° (wide-tele)
	Focal length	5.9mm to 147.55mm
	Focus	Auto, semi-auto, manual and rapid focus
	Zoom (speed)	Optical wide-tele: 4.8 seconds
Deep learning function	Face capture	Detection: up to 30 faces simultaneously. Supports detecting, tracking, capturing, grading, selection of face in motion and output of the best picture of the face.
	Perimeter protection	Line crossing, intrusion, region entrance and exit required. Support alarm triggered by specified target types (vehicle and human) required.
Events	Alarm linkage	Alarm actions: pre-set, patrol scan, pattern scan, memory card video record, trigger recording, notify surveillance centre, upload to FTP/Memory Card/NAS, send e-mail facility.
	Basic	Alarm input and output, exception, motion detection, video tampering alarm.
	Smart	Audio exception detection, intrusion detection, line crossing detection, object removal detection, parking detection, region entrance and exiting detection, unattended baggage detection, vandal-proof alarm.
	Smart tracking	Manual tracking, auto-tracking.
Illuminator	Smart supplement light capability	Required
	Supplement light type	Infra-red (IR)
	SL Range	Distance up to 400 metres
Image	Enhancement	BLC; HLC; 3d; DNR

	Privacy mask	Up to 24 masks, mosaic mask, polygon mask and mask colour configurable
	Regional exposure	Required
	Regional focus	Required
	Settings	Brightness, contrast, gain, saturation, sharpness, white balance adjustable through software and or web browser
	Stabilisation	Gyroscope capability required
	Wide Dynamic Range	140 dB
Interface	Alarm	7 inputs; 2 outputs
	Audio	1 line in: maximum input amplitude: 2-2.4 vpp with input impedance: 1 k $\Omega$ $\pm$ 10%. 1 line out: line level with output impedance: 600 $\Omega$
	Ethernet	1 RJ45 10M/100M self-adaptive port Hi-PoE
	On board storage	<ul style="list-style-type: none"> <li>Built-in memory card slot</li> <li>Up to 256 GB</li> </ul>
	RS-485	Contractor to state devices relevant to selected camera in his method statement.
	Video output	1.0V[p-p]/75 $\Omega$ ; PAL; NTSC; BNC connector
Network details	Application programming interface (API)	Contractor to state communication channels relevant to selected camera in his Tender.
	Council	
	Protocols	
	Security	<ul style="list-style-type: none"> <li>Full complicated password protection capability</li> <li>802.1x authentication</li> <li>Hypertext Transfer Protocol Secure – asymmetric encryption of communication</li> <li>Basic and digest authentication.</li> <li>Control timeout settings</li> <li>IP address filter</li> <li>Security audit logging facility</li> <li>Watermark</li> </ul>
	Simultaneous live view	Up to 20 channels

	User/host	Up to 32 users – levels: administrator; operator and user
	Web browser	Compatible with Chrome 57.0+, Safari 11+ and IE11.
Pan, Tilt, Zoom (PTZ)	Pan range / speed	360° / configurable: 0.1° to 210° per second; pre-set speed 280° per second.
	Tilt range / speed	-20° to 90° – auto flip / configurable: 0.1° to 150° per second; pre-set speed 250° per second.
	Park action	Auto scan, frame scan, panorama scan, patrol scan, pattern scan, pre-set, random scan, tilt scan.
	Patrol scan	8 patrols, up to 32 pre-sets for each.
	Pattern scan	4 pattern scans: recording time for each scan minimum of 10 minutes.
	3D positioning	Required
	Pre-sets	300
	Pre-set freezing	Required
	Proportional pan	Required
	PTZ status display	Required
	Power off memory	Required
	Scheduled task	Auto scan, aux output, dome adjust, dome reboot, frame scan, panorama scan, patrol scan, pattern scan, pre-set, random scan, tilt scan.
Road and vehicle traffic detection	Vehicle detection	Required – vehicle licence plate number; vehicle model; vehicle colour recognition.
Video	Main stream (frames per second)	50Hz: 25fps (1920 x 1080; 1280 x 960; 1280 x 720) 60Hz: 30 fps (1920 x 1080; 1280 x 960; 1280 x 720)
	Sub-stream	50Hz: 25fps (704 x 576; 640 x 480; 352 x 288) 60Hz: 30fps (704 x 480; 640 x 480; 352 x 240)
	Third stream	50Hz: 25fps (1920 x 1080; 1280 x 960; 1280 x 720; 704 x 576; 640 x 480; 352 x

		288) 60Hz: 30fps (1920 x 1080; 1280 x 960; 1280 x 720; 704 x 480; 640 x 480; 352 x 240)
	Video compression	Main stream: H.265+/H.265/H.264+/H.264 Sub-stream: H.265/H.264/MJPEG Third stream: H.265/H.264/MJPEG
	H.264	Baseline profile/Main profile/High profile
	H.265	Main profile
	RoI	8 fixed regions for each stream
	SVC	H.264 and H.265 encoding

- The cameras will be operated in accordance with our Data Protection Impact Assessment and our privacy statements for CCTV. A critical factor in protecting private spaces is all the cameras will have privacy masking techniques applied when operators scan a camera's range across residential dwellings etc. The privacy masking technique prevents the camera's view into people's windows etc.
- Security of the cameras and the network operation is of paramount importance. All NNC CCTV networks apply up-to-date and advanced network protection including authenticated access control. No single part of our networks are connected to the open internet or connected to unsecure channels etc.

## → AW1545/UP Cabinet Based Pole



AW1545/12/UP

**Fixed height range 4m - 15m**  
**Tilt Down height range 4m - 12m**

**Designed to meet the specific demands of urban area CCTV, our range of high specification cabinet based poles come as standard with venting, high security locks and high capacity, good quality, treated back boards. With many cabinet sizes, door options and head mounting options, backed up with a full range of accessories, the AW1545 UP pole range offers a comprehensive solution for urban CCTV installations.**

### Typically used for the following types of installation

- o Public area urban CCTV
- o Highways
- o Industrial and commercial premises
- o Schools and universities
- o Prisons and detention facilities
- o Utilities sites
- o Railway platforms & car parks
- o Car parks
- o Retail Parks
- o Sports stadia

### Security Features

- o Internal cabling
- o Close fitting flush doors
- o Solid secure heavy duty door locks and high security lock
- o Secure venting method
- o Internal padlock facility on tilt down poles to protect against un-authorized lowering
- o Anchor bolts below ground level

### General Features

- o Stable structures for all camera types
- o Available in 6 standard cabinet sizes, 300, 350, 400, 450, 500 and 600 square (400mm square as standard if not specified)
- o Flush fitting door, level with cabinet surface, no external frame combined with flush fitting Altron secure locks and a high security lock giving enhanced security and a clean aesthetic appearance
- o 4 point security door locking option
- o Standard convection venting eliminates condensation (when the pole base is properly sealed on installation)
- o Baffle vents to IP55 available as option
- o Demountable winches allow for a secure installation whilst also reducing costs on multiple installations
- o A wide range of standard Altron Accessories and Brackets available
- o Pole adaptations available to suit customers/project specific requirements
- o Constructed in high tensile steel and hot dip galvanised after fabrication for durability
- o Option of painting over the galvanised finish in colours available from BS and RAL colour charts
- o Also available in 316 stainless steel, architectural finish
- o For design, manufacturing and finishing standards, see details on page 107



AW1545/6TD/UP in tilted position

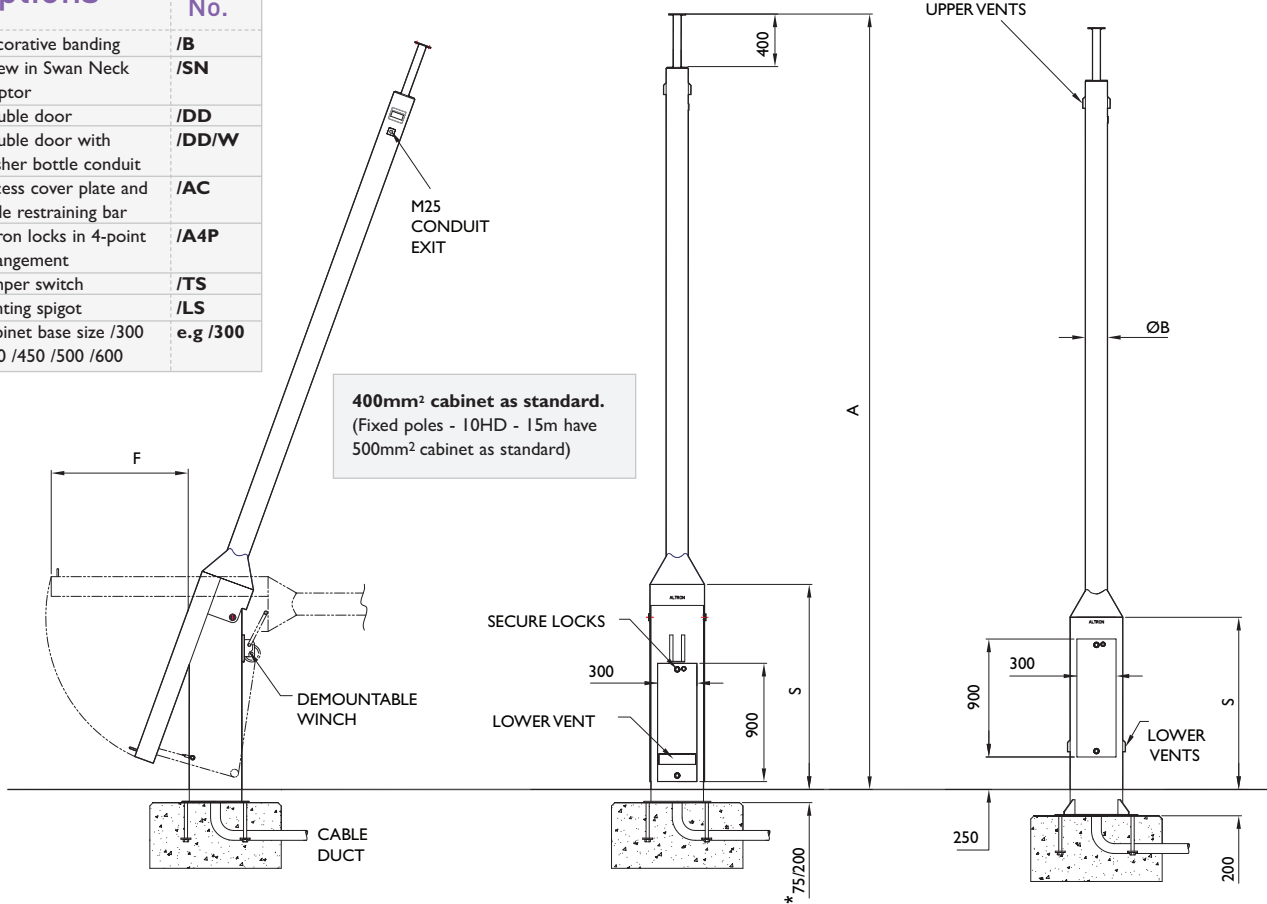


# → AW1545/UP Cabinet Based Pole Technical Specification

Options	PT No.
Decorative banding	/B
Screw in Swan Neck adaptor	/SN
Double door	/DD
Double door with washer bottle conduit	/DD/W
Access cover plate and cable restraining bar	/AC
Altron locks in 4-point arrangement	/A4P
Tamper switch	/TS
Lighting spigot	/LS
Cabinet base size /300 /350 /450 /500 /600	e.g /300

## AW1545UP TD

## AW1545UP



400mm<sup>2</sup> cabinet as standard.  
(Fixed poles - 10HD - 15m have 500mm<sup>2</sup> cabinet as standard)

Pole is fixed in the vertical position using 2 no. bolts and locked with internal nuts - has the facility to be padlocked internally to stop unauthorised tilting.

Poles complete with treated equipment mounting board inside compartment. Earthing lugs within pole & on door

All camera mounting plates are Ø 127 with 8 No Ø 8.5 equi-spaced on 101.6 PCD. Ø 40 thro' column spacer

\* 4-8m Tilt Down Units baseplate buried 75mm below ground level  
\* 10-12m Tilt Down Units baseplate buried 200mm below ground level

FOR FOUNDATION AND BOLTING DETAILS REFER TO PAGE 41

Model No.	Height in mtrs A	Max equip weight at top kgs	Max equip surface area m <sup>2</sup>	Pole ØB	Cabinet height above ground S	Pole rear clearance when tilting F	Winch part number	Product weight kgs
<b>AW1545UP-Fixed</b>								
AW1545/4/UP	4	40	0.25	168	1300	-	-	216
AW1545/5/UP	5	40	0.25	168	1300	-	-	238
AW1545/6/UP	6	40	0.25	168	1300	-	-	260
AW1545/7/UP	7	40	0.25	168	1300	-	-	292
AW1545/8/UP	8	40	0.25	168	1300	-	-	314
AW1545/8/UP/219	8	40	0.25	219	1300	-	-	350
AW1545/9/UP	9	40	0.25	219	1650	-	-	425
AW1545/10/UP	10	40	0.25	219	1650	-	-	496
AW1545/12/UP	12	40	0.25	273	1650	-	-	866
AW1545/15/UP	15	40	0.25	273	1650	-	-	995
<b>AW1545UP-Fixed Heavy Duty</b>								
Suitable for long offset arms or dual CCTV and lighting applications etc – or high rigidity								
AW1545/8HD/UP	8	80	0.5	219	1650	-	-	396
AW1545/10HD/UP	10	80	0.5	273	1650	-	-	780
<b>AW1545UP TD-Tilt Down</b>								
AW1545/4TD/UP	4	40	0.25	168	1625	1150	DW1000/45	246
AW1545/6TD/UP	6	30	0.25	168	1625	1150	DW1000/45	290
AW1545/8TD/UP	8	25	0.25	168	1625	1150	DW1500/45	335
AW1545/10TD/UP	10	40	0.25	219	2650	2150	DW2500/45	668
AW1545/12TD/UP	12	25	0.25	219	2650	2150	DW2500/45	726

Where payloads are greater than those stated above, please contact Altron  
All dimensions in mm unless stated otherwise

## Accessories

Top mounting brackets for Fixed and PTZ cameras	P76
Swanneck brackets for Dome cameras	P81
Anti-climb guards	P77
Clamp-on camera mounting brackets	P79
Telemetry box mounting brackets	P77
Pole top mounting cages	P83
PIR mounting ring	P84

## Quick reference

Single fixed camera knuckle	PTS-I
Twin fixed camera bracket	TB2-600F
Half swanneck for dome	AW1699H
Full swanneck for dome	AW1699F
Anti climb guard	SGC
PIR mounting ring	AW1962
Accessory bracket	ATBP