A blue and white crest with a horse and a ship

Description automatically generated

**STOURPORT-ON-SEVERN TOWN COUNCIL**

**CCTV Policy**

Status: Version 1.0

Date: 7th April 2025

Adopted:

To be Reviewed:

**1. Ownership**

* 1. Stourport-on-Severn Town Council operates CCTV surveillance systems (“the systems”) at the following sites;
* Riverside Toilets, Stourport-on-Severn
* Riverside Paddling Pool, Stourport-on-Severn
* Stourport Community Centre, Lickhill Road, Stourport-on-Severn

1.2 The systems monitor and records images. The systems are owned and managed by Stourport-on-Severn Town Council and operated by the Parks & Cemetery Superintendent and Assistant Clerk.

1.3 The responsible manager is the Town Clerk.

**2. Compliance**

2.1 Images obtained from the system which include recognisable individuals constitute personal data and are covered by the Data Protection Act 1998 and the EU General Data Protection Regulation 2018. This Policy should therefore be read in conjunction with the Town Council’s Data Privacy Notice.

2.2 The Town Council is the registered data controllers under the terms of the Act.

2.3 The Data Protection Officer for the Town Council is Susan Saunders (Town Clerk) who checks for ensuring compliance with the Act.

2.4 This policy has been drawn up in accordance with the advisory guidance contained within the Information Commissioner’s CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice.

**3. Purpose**

3.1 Stourport-on-Severn Town Council’s registered purpose for processing personal data through use of the CCTV system is public safety, crime prevention and investigating disputes. This is further defined as:

3.2 CCTV is used for the purposes of maintaining public safety, the security of property and premises and for preventing and investigating crime. It is not used to routinely monitor staff or councillors, but footage may be reviewed where an issue which may be contrary to safe working practices or contravenes the employee or councillor code of conduct is brought to the attention of the Town Clerk.

3.3 The information processed may include visual images, personal appearance and behaviours. This information may be about users of a site, the general public, contractors, staff or councillors. Information may only be shared with the Police or other law enforcement agencies if requested with good cause.

3.4 The operators of the system recognise the effect of such systems on the individual and the right to privacy.

3.5 Stourport-on-Severn Town Council is registered for CCTV under the data protection registration with the Information Commissioner’s Office number ZA444859.

**4. Description**

4.1 The systems are intended to produce images as clear as possible and appropriate for the purposes stated. The system is operated to provide when required, information and images of evidential value.

|  |  |
| --- | --- |
| Location |  |
| Riverside Toilets, Stourport-on-Severn | Four external cameras located in the following locations on the building:   * 1 x Above entrance door to ladies’ toilets * 1 x Above entrance door to men’s toilets * 1 x Looking along the front of the toilet block from the men’s toilets entrance * 1 x Looking along the front of the toilet block from the ladies’ toilets entrance   The cameras monitored |
| Riverside Paddling Pool, Stourport-on-Severn | Two external cameras located in the following locations:   * 1 x On left hand side of plant room looking towards paddling pool * 1 x On right hand side of plant room looking towards paddling pool |
| Stourport Community Centre, Lickhill Road, Stourport-on-Severn | 4 external cameras located in the following locations:   * 1 x on right hand side of the building (looking at the building from the car park) gable end (under the eaves) looking at the changing room/store doors * 1 x camera on right hand side of the building (looking at the building from the car park) gable end looking out over the car park. * 2 x cameras on the front of building. Looking at the building from the car park, one on the left hand corner of the building (under the eaves) looking out over the Car Park. Looking at the building from the car park, one on the right hand side of the building (under the eaves) looking out over the Car Park. |

**5. Operation**

5.1 Images captured by the systems are recorded continuously and may be checked by authorised staff via download to a computer. Images displayed on monitors will only be made visible to the operative downloading the footage. Only the Town Clerk, Parks & Cemetery Superintendent and Assistant Clerk may take recordings of CCTV images and recordings. Staff authorised to view CCTV are fully briefed and trained in all aspects of the operational and administrative functions of the relevant systems.

**6. Information Retention**

6.1 No more images and information shall be stored for more than 28 days, unless required for legal reasons. Images will be deleted once their purpose has been discharged.

**7. Access**

7.1 All access to recorded images is recorded in the daily log. Access to images is restricted to those who need to have access in accordance with this policy. Disclosure of recorded material will only be made to third parties in accordance with the purposes of the system and in compliance with the Data Protection Act.

7.2 Anyone who believes that they have been filmed by the system can request a copy of the recording, subject to any restrictions covered by the Data Protection Act (“Subject access request”). Data subjects also have the right to request that inaccurate data be corrected or erased and to seek redress for any damage caused.

7.3 Procedures are in place to ensure all such access requests are dealt with effectively and within the law.

7.4 Access requests should be sent by letter to:

Stourport-on-Severn Town Council

First Floor, Civic Centre

New Street

Stourport-on-Severn

Worcs DY13 8UN

**8. Feedback**

8.1 Members of the public should address any concerns or complaints over use of Stourport-on-Severn Town Council’s CCTV system to stourporttown.clerk@stourporttowncouncil.gov.uk or by telephone to 01562 732750.

**9. Annual Review**

9.1 This policy will be reviewed annually by the Parks Committee to ensure that the purpose still applies.

**10. Legal Basis for Processing Personal Data**

10.1 One of the seven major data processing principles of GDPR is to ensure that personal data is processed lawfully, fairly, and transparently. To comply with this principle, Chapter 6 of the GDPR requires any organisation processing personal data to have a valid legal basis for that personal data processing activity. GDPR provides six legal bases for processing:

Consent – The data subject has given permission for the organisation to process their personal data for one or more processing activities. Consent must be freely given, clear, and easy to withdraw, so organisations need to be careful when using consent as their legal basis.

Contract – The data processing activity is necessary to enter into or perform a contract with the data subject. If the processing activity does not relate to the terms of the contract, then that data processing activity needs to be covered by a different legal basis.

Legitimate Interest – This is a processing activity that a data subject would normally expect from an organisation that it gives its personal data to do, for example marketing activities and fraud prevention. Public authorities cannot use legitimate interests as a lawful basis if the processing is in the performance of tasks as a public authority.

Vital Interest – A rare processing activity that could be required to save someone’s life. This is most commonly seen in emergency medical care situations.

Legal Obligation – The processing activity is necessary for a legal obligation, such as on information security, employment or consumer transaction law.

Public Interest – A processing activity that would occur by a government entity or an organisation acting on behalf of a government entity.

10.2 The ICO office asks that operators consider the justification of CCTV in the positions in which it is implemented and review this on an annual basis. The following justification is based on a lawful basis and legitimate interest as defined by the ICO.

|  |  |
| --- | --- |
| **Area** | **Lawful Basis** |
| Riverside Toilets, Stourport-on-Severn | Public Interest (public and employee safety, prevention and protection of crime) |
| Riverside Paddling Pool, Stourport-on-Severn | Public Interest (public and employee safety, prevention and protection of crime) |
| Stourport Community Centre, Lickhill Road, Stourport-on-Severn | Public Interest (public and employee safety, prevention and protection of crime) |

**Checklist for users of limited CCTV systems monitoring small retail and business** premises.

This CCTV system and the images produced by it are controlled by Stourpot-on-Severn Town Council who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1988).

Stourport-on-Severn Town Council has considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of the public, our employees and users of our owned and managed facilities. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Checked (Date)** | **By** | **Date of next review** |
| Notification has been submitted to the Information Commissioner and the next renewal date recorded |  |  |  |
| There is a named individual who is responsible for the operation of the system |  |  |  |
| Prior to processing, we have clearly defined the problem we are trying to address. We regularly review our decision to use a surveillance system. |  |  |  |
| We have identified and documented an appropriate lawful basis for using the system, taking information into consideration Article(s) 6, 9 and 10 of the UK GDPR and relevant Schedules of the DPA 2018. |  |  |  |
| Our system produces clear images which we can easily disclose to authorised third parties. For example when law enforcement bodies (usually the police) require access to investigate a crime. |  |  |  |
| We have positioned cameras in a way to avoid any unintentional capture of private land or individuals not visiting the sites. |  |  |  |
| There are visible signs showing that CCTV is in operation. Contact details are displayed on the sign(s) if it is not obvious who is responsible for the system. |  |  |  |
| We securely store images from this system for a define period and only a limited number of authorised individuals may have access to them. |  |  |  |
| Our organisation knows how to respond to individuals making requests for copies of their own images or for images to be erased or restricted. If unsure, the controller knows to seek advice and guidance from the Information Commissioner’s Office (ICO) as soon as a request is made. |  |  |  |

**The guiding principles of the Surveillance Camera Code of Practice.**

System operators should adopt the following 12 guiding principles:

1. What’s your system for? Do you review its use?
2. Have you carried out a privacy impact assessment? Do you publish your privacy impact assessment?
3. Do you have signage in place to say surveillance is taking place? Is there a published point of contact for people to raise queries or complaints with?
4. Who’s responsible for your system? Are your staff aware of their responsibilities?
5. Do you have clear policies and procedures in place? Do you staff know what your policies and procedures are?
6. How long do you keep images/information? How do you make sure images/information is deleted once they’re no longer needed?
7. Do you have a policy on who has access to the stored information? Do you have a policy on disclosure of information?
8. Do you follow any recognised operational or technical standards?
9. Do you make sure that the images captured by your system are caught securely? Are only authorised people given access to the images?
10. Do you evaluate your system regularly to make sure it’s still required? Could there be an alternative solution to a surveillance camera system?
11. Can the criminal justice system use the images and information produced by your surveillance camera system? Do you have a policy on data storage, security and deletion?
12. Do you use any specialist technology such as ANPR, facial recognition, Body Worn Video (BWV) or remotely operated vehicles (Drones)? Do you have a policy in place to ensure that the information contained on your database is accurate and up to date?