

Service Level Agreement

Between

Gloucestershire Constabulary

and

[insert Community / Parish details]

Agreement Date: [insert date]

Contents

Definitions	Page 3
Purpose and scope	Page 4
Duration	Page 4
Obligations	Page 5
Funding	Page 6
Staffing	Page 6
Security	Page 6
Record keeping	Page 6
Monitoring and review	Page 6
Termination	Page 6
Effect of termination	Page 7
Indemnity	Page 7
Confidentiality	Page 7
General clauses	Page 7
Appendix A	Page 8
Appendix B	Page 12
Appendix C	Page 12

THIS AGREEMENT dated the **[insert date]** is made between
Gloucestershire Constabulary and **[insert Community / Group]**

1. Definitions

- 1.1 **“Agreement”** - this Agreement between Gloucestershire Constabulary and the Community and / or Parish to provide and operate a **Community Speed Watch +** system and process.
- 1.2 **Appropriate technical device** – Surveillance Camera Commissioner(SCC) approved road side image capturing device system.
- 1.3 **Community Speed Watch +** – Community Speed Watch activities centred around an **appropriate technical device system**.
- 1.4 **Community Speed Watch** – a national initiative where, in partnership with the police, members of the communities use detection devices to monitor local vehicle speeds. The community members record and report drivers exceeding the speed limit to the police with the aim of educating drivers to amend the driver behaviour.
- 1.5 **Data Controller** – is a person, public authority, agency or other body which alone, or jointly with others, determines the purpose and means of processing personal data. In other words, the data controller determines the “why” and “how” personal data is processed.
- 1.6 **Data Processor** – processes personal data on behalf of the controller. The data processor is usually third party with no direct / organisational link to the data controller.
- 1.7 **DPA** – Data Processing Agreement, is an agreement between a data controller and a data processor, it regulates any personal data processing conducted for business purposes. A DPA may also be called a GDPR data processing agreement.
- 1.8 **DPIA** – Data Protection Impact Assessment describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. *DPIAs are an important tool for negating risk and for demonstrating GDPR compliance.*
- 1.9 **GDPR** – The General Data Protection Regulation is Europe’s replacement framework for data protection laws, replacing the UKs 1998 Data Protection Act. The UK’s decision to leave the European Union has not altered this. GDPR sets out requirements for how organisations handle personal data.

- 1.10 **Personal Data** – means any information relating to an identified or identifiable individual. An identifiable individual is a person who can be identified directly, or indirectly, in particular to an identification number (for example National Insurance number, vehicle registration number). It is also relevant to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity (for example name, first name, date of birth, biometrics, fingerprints, DNA).
- 1.11 **Relevant Authority** – are a list of authorities that fall under the guidance set out by the Surveillance Camera Commissioner (SCC). The list includes Local Authorities, Parish Councils, the Office of Police & Crime Commissioner and any Chief Officer of a Police Force in England and Wales.
- 1.12 **Surveillance Camera Commissioner** – the role of the Surveillance Camera Commissioner (SCC) is to encourage compliance with the Surveillance Code of Practice. The office of the SCC was created under the Protection of Freedoms Act 2012 to further regulate CCTV. It does not have enforcement powers, however noncompliance with SCC guidance can (and has) been admitted in relevant Civil and Criminal Court proceedings. The SCC Code of Practice is set around 12 “Guiding principles” (**see Appendix A**).

2. Purpose and Scope

2.1 This Agreement represents commitments:

- By Gloucestershire Constabulary to support **CSW+** activities by acting as data processors in accordance with the terms of this Agreement;
- By the **CSW+** group to operate and administer **CSW+** activities in accordance with the terms of this Agreement; and
- By both parties to monitor and review the performance of **CSW+** and to seek ways of ensuring that it operates for the benefit of the local community whilst abiding to the principles set out within the SCC Code.

3. Duration

1. This Agreement is ongoing and remains valid subject to review of need. Throughout the term of this Agreement, Gloucestershire Constabulary and the **CSW+** group will monitor results at the chosen locations to satisfy themselves that there remains a specific issue with speeding. A cessation in speeding incidents will remove the requirement for an image capturing device used for CSW+ activities regardless of the agreed review date. On the basis of an annual review, Gloucestershire Constabulary will use this information and any further information

submitted by the **CSW+** group to decide whether it wishes to continue supporting **CSW+** activities.

2. Gloucestershire Constabulary will provide 28 days' notice (in writing) should it decide not to renew its support of **CSW+** activities.
3. Individual **CSW+** groups will be required to make payment for 2nd class postage costs incurred by Gloucestershire Constabulary when letters are created and posted to registered keepers of vehicles that are highlighted by **CSW+** activities. Numbers of letters posted per **CSW+** group will be agreed between each group and Gloucestershire Constabulary. Invoicing on a quarterly basis with costs subject to annual review. Initial agreements will be for 10 registration numbers per camera per week, this will be subject of annual review.
4. Image capturing device systems operated by **CSW+** groups must be **SCC accredited** at the point of purchase and compliance must be maintained for the duration of **CSW+** activities (the supplier will be able to demonstrate evidence of accreditation by production of an accreditation certificate).
5. In the interests of proportionality and necessity the data controller/s will ensure stored personal data is expunged every 12 months.

4. Obligations

- 4.1 The **CSW+** group is responsible for safeguarding the physical condition of the image capturing device.
- 4.2 The **CSW+** group maintain responsibility for meeting requirements laid down by Gloucestershire County Council (GCC) when using GCC road side furniture for housing the image capturing device.
- 4.3 All parties involved with **CSW+** activities will operate within the principles of GDPR.
- 4.4 Each **CSW+** group will produce a DPIA for activities in their area (the device suppliers will have produced a DPIA for their devices).
- 4.5 Gloucestershire Constabulary will action intelligence that is generated by **CSW+** activities in a way that the Constabulary feels most appropriate, the aim being to geographically target persistent excess speed activity. Gloucestershire Constabulary will also aim to target specific offending vehicles, identified by communities, that are routinely used in the commission of road traffic offences or are used in committing more serious offences.
- 4.6 Gloucestershire Constabulary to review letter pricing, based on second class post, annually, the timing of which will be reliant on Royal Mail

costing notification and aimed at assisting with any planned budget setting.

- 4.7 Each CSW+ group will send one spreadsheet per camera each week in the format supplied by Gloucestershire Constabulary.
- 4.8 Gloucestershire Constabulary to send letters within one working week of receipt of data.

5. Funding

- 5.1 **CSW+** groups are responsible for funding their own or securing funding for the procurement of image capturing devices.

6. Staffing

- 6.1 **CSW+** groups will be responsible for staffing all back end functions as a part of their role/s as data managers (including data management and intelligence sharing). Gloucestershire Constabulary will perform functions as data processors and also perform joint site surveys with GCC.
- 6.2 **CSW+** groups will ensure that it provides a safe environment for its volunteers.

7 Security

- 7.1 CSW+ groups are responsible for taking reasonable measures to ensure the security of the image capturing devices and any signage associated with CSW+ activities. Any loss and / or thefts should be reported to Gloucestershire Constabulary.

8. Record Management

- 8.1. For the purposes of GDPR, data includes hand written notes, printouts and hard copies of data. All data records should be managed in accordance with GDPR principles.
- 8.2. Data transfer (into Gloucestershire Constabulary) should be via XLS file transfer and email.

9. Monitoring and Review.

- 9.1 The Service can be reviewed jointly by the CSW+ group, GCC and Gloucestershire Constabulary by mutual consent. The areas that will form the basis of the monitoring and review appear in **Appendix D**.

10. Termination

- 10.1 If at any time either party wishes to terminate the Agreement, it may do so by giving each party 28 days' written notice
- 10.2 The Agreement will also terminate at the end of the current term if it has not been reviewed in accordance with **Appendix D** or monitored for continued requirement in accordance with paragraph 3.1

11. Effect of Termination

- 11.1 If data collection continues after the termination period this could be held as disproportionate and in breach of SCC guidance.

12. Indemnity

- 12.1 **CSW+** groups shall indemnify Gloucestershire Constabulary completely against any claims, costs, demands or judgements which result from CSW+ activities unless such claims, costs, demands or judgements result from the Constabulary's own negligence.
- 12.2 Gloucestershire Constabulary shall indemnify the **CSW+** groups completely against any claims, costs, demands or judgements which result from carrying out any instruction issued by the Constabulary unless such claims, costs, demands or judgements result from the **CSW+** groups own negligence.

13. Confidentiality

- 13.1 Neither of the parties nor their agents, staff or representatives shall during this Agreement and after it has been terminated use or disclose to any person who has no right to receive it, any Confidential Information which comes to the knowledge of the other party as a result of being involved in the making and implementation of this Agreement and **CSW+** activities. If one party is unsure as to whether or not a particular piece of information is confidential it shall check in writing its status with the other party before disclosing it to a third party.

14. General Clauses

- 14.1 No amendment to this Agreement shall be valid unless it is agreed by both parties and evidenced in writing.
- 14.2 The invalidity, illegality or unenforceability of any term or condition shall not affect the validity, legality or enforceability of any other term or condition used in this Agreement.

14.3 This Agreement shall not create any rights for the benefit of or enforceable by any person who is not a party hereto. The provisions of the Contracts (Rights of Third Parties) Act 1999 are expressly excluded.

14.4 This Agreement shall be construed in accordance with English law and the parties hereby submit to the exclusive jurisdiction of the English Courts.

IN WITNESS whereof the parties have signed this Agreement the day and year first before written

SIGNED: _____
For an on behalf of the **CSW+** group

NAME _____
(Please print)



SIGNED: _____
For and on behalf of Gloucestershire Constabulary

NAME __Robert Vestey_____
(Please print)

Appendix A

SCC Code including its 12 Guiding Principles Police advice.

Appendix B

Copies of **CSW +** letters (to vehicle registered keepers).

Appendix C

Monitoring and review process

Appendix A

SCC 12 Point Code – Guidance notes from John Lynch-Warden

The “Surveillance Camera Commissioner Code (SC Code) CC CODE” sits under Section 29 to 31 of the Freedom of Information Act 2012. It is not a separate piece of legislation. The 2012 Act covers a vast array of personal data / information management legalities. It was the 2012 Act that directed the Surveillance Camera Commissioner to produce a Code of Practice, which more recently has been expanded to include bio-metrics. The Code is based on 12 Guiding principles.

The important points to be aware of -

This is not mandatory or fixed in statute, however it is good practice that the SCC encourages. The Code makes it clear that failure to comply with these principles can be used in both Civil and Criminal proceedings where there has been a data breach. There are marketing advantages to being compliant, covered later in these notes.

The SCC Code doesn't only apply Community Speed watch devices, it also includes CCTV, Body Worn Video, ANPR etc. All surveillance camera systems regardless of whether there is live viewing or recording of images, or information associated with data are included.

The SCC Code only applies to devices used in **public places**, and only applies to the **Police** and other “**Relevant authorities**”.

Relevant Authorities include -

- A Local Authority as defined by the Local Government Act 1972 (District Councils, Parish Councils, Highways Authorities to name but a few).
- Office of Police and Crime Commissioner.
- Any Chief Officer of Police in England and Wales.

Covert Surveillance is not covered by this SCC Code – this is covered by the Regulation of Investigatory Powers Act 2000.

The SC Code sets out 12 guiding principles which strike a balance between protecting the public and upholding civil liberties.

The principles exist to provide a coherent and comprehensive structure that enables good, transparent decision-making, and will reassure the public that surveillance cameras are used to protect and support communities rather than spy on them (this is where necessity, proportionality and transparency comes from).

Cameras cannot be covert, there should be signage to show that cameras are in use, and they should be for a specific purpose (eg. road safety/speeding).

There must to be a specific purpose. Once the specific purpose has ceased, then the requirement for the camera would also have ceased as it would no longer be proportionate, necessary etc.

The 12 Guiding Principles –

The SCC accepts that full adherence to each element of these principles may not be relevant to every camera system but you should be able to demonstrate that they have been considered.

1. 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. *What is your system for? • Its use will require regular review.*
2. 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. *Do you publish your privacy impact assessment?*
3. 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. *Is there signage and a published point of contact for people to raise queries or complaints?*
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used. *Are your staff, employees, processors and data owners each aware of their responsibilities?*
5. 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. *Do staff know what your policies and procedures are?*
6. 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. *How do you ensure images/information are deleted once they are no longer needed?*

7. 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. *Suppliers and data owners would have to demonstrate they have relevant policies in place.*

8. 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. *Suppliers should comply with relevant standards for the industry.*

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use. *Only authorised people should be given access to the images/data.*

10. 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. *Why is it still required? Could there be an alternative solution to a surveillance camera system?*

11. 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. *Do you have a policy on data storage, data sharing, security and deletion?*

12. 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. *Do you have a policy in place to ensure that the information contained on your database is accurate and up to date?*

The guidance is open to interpretation and is not specific in some areas. An example of this is in relation to the positioning of cameras and their justification. Whilst there is no absolute requirement for accreditation to be location specific, there is a requirement to follow the above principles as cameras need to be for a specific purpose and once this purpose is no longer relevant (i.e. speeding is no longer an issue), then the requirement for a camera at that location ends. It would be a breach of the Code to retain a camera that captures personal information at a location where there was no specific purpose for it.

The SCC provides an on-line self-assessment tool to help organisations and suppliers test themselves against these guiding principles.

Following on from the 12 principles and the self-assessment is a certification process that enables organisations and suppliers to be audited with the view to receiving a certification mark and a certificate issued by the Biometrics and Surveillance Camera Commissioner. This is not a legal requirement and not legally enforceable but will help to raise standards in the industry and enable organisations to demonstrate compliance with the code. It also affords protection to all parties involved in the process.

The SCC Code explains in detail how to follow the certification process. The surveillance camera certification process is available for any organisation that operates surveillance in a public space. The code explains that this could be a small or large organisation that wants to demonstrate as part of its public accountability arrangements how it has complied with the Surveillance Camera Code of Practice. Certification is primarily for those that must have regard to the code – the regulated sector – in particular local authorities and Police who own or operate a large proportion of the systems within the regulated sector.

Bodies that achieve certification will receive a certificate (and should be able to produce it on request) from the Biometrics and SCC Office and so will be able to use the SCC certification mark on their web site and other marketing materials. A list of bodies who have achieved this standard also appears on the SCC Web site. This in itself is a selling point for suppliers who operate in an increasingly crowded market. It also serves as a reassurance that the use of such devices is ethical, monitored and scrutinised.

Certification lasts for 5 years, there is an annual inspection to ensure continued compliance and maintenance of standards.

Appendix B:



CES_LETTER1.docx



CES_LETTER2.docx

Appendix C:

1. The monitoring and review process will be a joint activity between the **CSW +** group and Gloucestershire Constabulary with the aim of ensuring:
 - the best service possible to customers
 - the most effective use possible of the resources available and value for money.
 - that is compliant with GDPR principles and SCC Guidance.
 - Each **CSW+** group will have a nominated point of contact.
2. Both the **CSW+** groups and Gloucestershire Constabulary wish to ensure that the arrangements set out in the Agreement work smoothly, and that improvements to the service to customers can be made wherever possible. A further key element of the review process, therefore, will be to monitor the efficient working of these processes to identify problems and improvements and to act on this wherever possible.
3. The review will be an annual event and
 - Clarify whether or not the speeding problem still exists where the cameras are located.
 - Articulate any reduction in overall speeding.
 - Highlight any complaints of data breaches and what was put in place to resolve.
 - Form an agreement between both parties for the activity to cease or continue.