Privacy Impact Assessment – Version 1.0 Chelmsford City Council (SEPP)

This form is designed to help you carry out a high-level Privacy Impact Assessment (PIA). A PIA is a risk assessment for personal information, and is carried out as part of our compliance with the Data Protection Act and associated guidance from the Information Commissioner. The PIA will enable you to identify whether your project or system is likely to have an impact on the security of such information. The term 'system' includes any way of working – not just computer use – for example a manual filing system.

Using a PIA early in a project or system design will help to identify potential problems so that you can address them and take extra steps to protect information where needed. If after using this form there are indications of a significant impact on the way personal information is held and used, it may be necessary to do a more thorough assessment looking at each requirement of the Data Protection Act in detail.

You may not be able to complete the assessment in full early in the project, but you can update it later when the information is available. Where issues are identified, you should review the form later, for example before implementation, to ensure they have been addressed.

The Home Surveillance Commisioner has issued a Surveillance Camera Code of Practice which is our reference and we will be working with them to look at any areas of doubt and they will retain a copy of the completed assessment.

The camera hardware and software supplier is Reveal Media and we will be working with them to look at any areas of doubt and use their industry knowledge and experience.

Name of project: SEPP - Civil Enforcement Officer Body-worn Camera	**Name of officer**: Russell Panter
Department (or lead department): Community Services	**Date form completed**:
Date form reviewed:	**Name of officer**:

Ref.	Question	Answer	Notes
1.1	Have you identified an Information Asset Owner, and if so, who is it?	Parking Partnership Manager	Each asset should be owned
1.2	Is the system being supplied and/or supported by a third party, and if so, how will their access to personal information in the system be controlled and monitored?	Support and software supplied by Reveal Media Ltd. who will have no access to any information retained by Chelmsford City Council	Companies who maintain systems may have to connect remotely in order to fix problems, apply upgrades etc.
1.3	If information will be processed by a third party, is there, or will there be, a contract in place?	In house	All processing will be done in-house.
1.4	If information will be processed by a third party, is there, or will there be, an agreement which defines how they will protect the information?	In house	Consider not only day-to-day processing but one-off requirements such as data scanning and conversion.
1.5	If a computer system is being hosted by a third party, is the data being held within the EEA or in a country where the arrangements have been assessed as being adequate?	Hosted on a non-networked site specific PC	Data Protection Act 1988, eighth principle. Data held outside the European Economic Area requires assessment.
1.6	If a system is replacing something else, what is happening to the old system or paper?	This is an entirely new system	Secure archiving, storage or disposal may be required.
1.7	Does the system use identity management for citizens or other users, involving the authentication of the user through a token or other means? If so, have any concerns been fully investigated?	N/A	Automatic user recognition carries the potential for data loss through mistaken identification, and also for significant public concern over this. Consider too the security of original documents presented for identification purposes.
1.8	Does the system use new technologies of which the user may be suspicious, and if so, have sufficient time and resources been allocated to addressing this and allaying any concerns?	N/A	E.g. smart cards, RFID tags, biometrics, GPS and locators, image and video recording, and profiling. Technology which can bee seen as intrusive generate public concern, and are a project risk.
2.1	If information will be held on paper (including prior to data entry) are the storage and disposal arrangements sufficiently secure?	Yes, incident forms.	Include consideration of office arrangements whilst documents are waiting or being processed.
2.2	If paper documents are being scanned into a system, is this done by the Post Room and then held securely? If not, has the risk of them being inadmissible in court been assessed?	N/A	If documents may be needed in court proceedings we must scan and hold them in a way which preserves their integrity to the court's satisfaction.
2.3	Will there be any adverse changes to the way records are handled, such as their version control, retention or archiving?	No	Future consideration required if changes are made.

Ref.	Question	Answer	Notes
2.4	Does the new system hold documents in a document management system, and if so, is any adjustment needed to the file plans?	No	
3.1	Is the system protected from unauthorised access through the council's network?	System is Password Protected. All footage is held and controlled within a secure software package.	Consider access hierarchy.
3.2	Is the system protected from unauthorised access through Internet?	Yes	System may be networked in future so IT considerations required.
3.3	Is the system adequately protected from accidental loss of information (database, paper, backups etc.)?	Yes	Consider when backups are taken and how much work will need to be re-done in the event of a loss Consult Business Improvement and/or ITSD.
3.4	If the system can be accessed remotely, are measures to protect sensitive information adequate and do they meet the requirements of the IT Policy?	Not networked	Consider whether data can be transferred to remote computers i.e. Police or courts
3.5	How will you ensure that staff using the system are adequately trained in both the system itself and in information security, and that this training is kept up to date and refreshed?	Only the Parking Enforcement Manager and 2 Team Leaders will have access to system. All have received training in system use and data protection/security.	Consider both existing and new staff.
3.6	Are there sufficient controls over who can administer and use the system, and will administrators be suitably authorised and trained?	Yes	
3.7	If the system is accessible over wireless technology, are there sufficient controls to prevent access except from authorised devices?	N/A	Consider public Wi-Fi and personal devices, whether laptops or hand-held devices. Seek assurances from IT Service Delivery if required.
3.8	If the system uses a shared password are there adequate arrangements to change it frequently and after staff changes?	All usernames and passwords are unique and will be deleted as soon as soon as staff leave.	No shared passwords
4.1	Will personal data be handled in a different way, that could mean it is linked to or matched with other data, requiring a review of how it is protected?	No	Data Protection Policy
4.2	If personal data will be handled in a different way, is the justification for doing that completely clear?	N/A	
4.3	Are you satisfied that Chelmsford City Council will be able to meet its obligations in respect of file access requests?	Yes	Subject Access Requests are part of the Data Protection Act 1998 (section 7)

Ref.	Question	Answer	Notes
4.4	Will the system attach a person's identity to information which would previously have been anonymous? If so has the potential for loss of privacy been investigated?	No	If data has previously been used in an anonymous way, any conversion to identifiable data will cause privacy concerns.
4.5	If the system holds sensitive personal data which merits special protection, have checks been made to ensure that this protection is present and consistent?	N/A	Section 2 of the DPA identifies categories of sensitive personal data including racial & ethnic origin, political opinions, religion, union membership, health, sexual life, offences and court proceedings.
4.6	If the system holds information about vulnerable people, have suitable measures been taken to protect that information?	N/A	The impact of the loss of information about vulnerable people is sufficient to warrant additional protection and checks.
5.1	If Chelmsford is not the Data Controller and Data Processor for the information, is it clearly agreed and documented who carries out these roles?	In house	See the Data Protection Act 1998.
5.2	If the system will use any data from other councils or organisations, are the necessary information sharing arrangements in place and documented?	N/A	May need considerations if a future partnership is set up.
5.3	If the data will be used in different parts of the council, are you satisfied that it is only being used for the purposes for which it was originally collected?	N/A	Data Protection Act 1998 – 2nd principle. Information sharing pages
5.4	Have arrangements been made for routine transfers of information to be carried out securely, and if so, how will this be done?	Any data for police use will be burned onto a hard disk and once handed to them will fall within the police data protection policy. No transfer of data to take place across a network.	Standard email and internet services between organisations must be regarded as insecure. Security covers loss, corruption and unauthorised access.
5.5	Could the linking of information across different systems make data become accessible when it should remain protected? If so, are you satisfied that adequate measures are in place to protect the data?	N/A	
6.1	Have arrangements been made to assure the quality of the information being added to the system, both at take-on and daily?	N/A	Suitable measures can include validation routines, spelling checks, verification and sign-off of data.

Ref.	Question	Answer	Notes
6.2	Will processes be in place to ensure that there are no inconsistencies with data held in other systems, whether manual or otherwise?	N/A	It is good practice to hold data only once if possible, and access it as required.
7.1	Are you satisfied that the information held will still be accessible when required to answer Freedom of Information (FOI) requests?	All details of saved data are contained in the Information Asset Log, including officer number, date and location of incident. Data will only be retained until investigations have taken place or prosecutions completed. All other data will be deleted.	Timely responses to requests are required by law (Freedom of Information Act 2000)
7.2	Have arrangements been made where appropriate to produce information for publication under Open Data requirements?	N/A	This information is published on the web site.
7.3	Will there be any changes to the publication scheme as a result of this project?	N/A	The publication scheme lists the information that we publish, or intend to publish, routinely. Doing this is a good way to avoid FOI requests.

This space is available to record any concerns arising from the assessment, and the action being taken to address them:

Ref.	Concern	Date	Action	Resolution	Date