Privacy Impact Assessment – Version 1.0 Cambridge City Council

Name of project: Body Worn Camera for Public Realm Enforcement Officers and the Dog Warden Service	**Name of officer:** Tom Pickover
Department: Streets and Open Spaces	**Date form completed: 1 August 2016**
Review date:	**Reviewing officer:**

This form is designed to help you carry out a Privacy Impact Assessment (PIA).

A PIA is a risk assessment helps to assess privacy risks to individuals in the collection, use and disclosure of personal information. This 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.

Using a PIA early in a project will help identify potential problems so you can address then and take additional steps to protect information where needed.

The Information Commissioner has published a Code of Practice on conducting PIAs.

Reference.	Question	Answer	Notes
1	**Information Systems**		
1.1	Have you identified an Information Asset Owner, and if so, who is it?	Wendy Young, Operations Manager (Responsible Officer).	
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	Support and software supplied by XYZ	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?	N/A.	A contract is a basic requirement for all processing
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?	N/A.	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?	N/A - The system is locally hosted on CCC systems	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.
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?	Staff using this system to undertake training and to be consulted on impacts of using the system.	E.g. smart cards, RFID tags, biometrics, GPS and locators, image and video recording, and profiling. Technology which can be seen as intrusive generate public concern, and are a project risk.

Reference.	Question	Answer	Notes
2	**Information Systems**		
2.1	If information will be held on paper (including prior to data entry) are the storage and disposal arrangements sufficiently secure?	Yes.	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 – Records will be handled in accordance with the operational procedure and adhere to the advanced safeguards in place.	records-management-main-page.
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.	The file plan needs to reflect the document types in use and to what extent they are available

Reference.	Question	Answer	Notes
3	Security		
3.1	Is the system protected from unauthorised access through the council's network?	The system is Password Protected. Any retained information will be kept on encrypted external hard drives kept in secure conditions.	Consider system access controls and permissions on files and folders. Consult Business Improvement and/or ITSD.
3.2	Is the system protected from unauthorised access through Internet?	Yes – The system will be protected through Cambridge City Council's computer system's security.	Consider whether external access is through a secure route, PSN etc.
3.3	Is the system adequately protected from accidental loss of information (database, paper, backups etc.)?	Yes - Images will be stored on a securely stored external hard drive. Images will be backed up on another securely stored external hard drive stored at a separate location. All hard drives will be kept securely in evidence rooms, and access will be logged to prevent unauthorised access/removal from office.	Consider when backups are taken and how much work will need to be re-done in the event of a loss.
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?	N/A.	Consider whether data can be transferred to remote computers or sensitive documents kept at home.
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?	All system users will have received training in system use and data protection/security. Training will be recorded centrally and refresher training will be provided to staff annually.	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 - Only the Public Realm Enforcement and the Dog Warden service will have access to the system.	Consider whether administration is done by IT Service Delivery or the user department, access controls etc.

Reference.	Question	Answer	Notes
4	Personal data handling		
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?	Personal data will be held in line with CCC's Data Protection Policy.	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.	Users are more likely to accept new or revised processes if they can see the benefits. Vague justifications such as 'for security reasons' are unlikely to suffice.
4.3	Are you satisfied that Cambridge City Council will be able to meet its obligations in respect of file access requests?	Yes - Subject Access and information sharing with other agencies is detailed in the operational procedure.	Subject Access Requests are part of the Data Protection Act 1998 (section 7)
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.

Reference.	Question	Answer	Notes
5	Multiple organisations and systems		
5.1	If Cambridge City Council is not the Data Controller and Data Processor for the information, is it clearly agreed and documented who carries out these roles?	N/A.	See the Date 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.	Information Sharing Agreements are used to define the parameters under which information can be shared. Information sharing pages
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?	Yes - There will be times when information is shared internally between different departments. The sharing of this data will be in line with the original purpose or in the exercising of data subjects rights.	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?	Yes – Secure transfer of recordings will be made by the EO to CCC IT systems and copies backed up on encrypted external hard drives. Any other data, not required for evidential purposes, will be deleted by the EO by the next working day.	Standard email and internet services between organisations must be regarded as insecure. Security covers loss, corruption and unauthorised access. See Transferring Information
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.	The trend towards joined up services could mean that staff in one team gains access to information about a person that they have no right to see, for example tax arrears or parking issues.
5.1	If Cambridge City Council is not the Data Controller and Data Processor for the information, is it clearly agreed and documented who carries out these roles?	N/A.	See the Data Protection Act 1998.

Reference.	Question	Answer	Notes
6	Data Quality		
6.1	Have arrangements been made to assure the quality of the information being added to the system, both at take-on and daily?	Yes - To ensure compliance with the Data Protection Act, CCC's BWC CCTV systems are subject to the Council's Operational Procedure, Code of Practice and Privacy Impact Statement.	This is addressed in s2.5 of Annex A and section 3 of the Operational Procedure. Suitable measures can include validation routines, spelling checks, verification and sign-off of data.
6.2	Will processes be in place to ensure that there are no inconsistencies with data held in other systems, whether manual or otherwise?	Yes - The system will provide unique metadata for each recording.	It is good practice to hold data only once if possible, and access it as required.Transparency and open data | CityNet Information Governance Policy | CityNet
7	Information governance		
7.1	Are you satisfied that the information held will still be accessible when required to answer Freedom of Information (FOI) requests and data subjects rights under DPA such as Subject Access.	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 immediately.	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?	Data is not suitable for publication under Open Data.	This information is published on the web site on the Open data: Transparency in local government | Cambridge City Council
7.3	Will there be any changes to the publication scheme as a result of this project?	No.	The publication scheme lists the information that we publish, or intend to publish, routinely. Doing this is a good way to avoid FOI requests.