RIBBLE VALLEY BOROUGH COUNCIL

PRIVACY IMPACT ASSESSMENT (PIA) FOR

RIBBLE VALLEY BOROUGH COUNCIL

CLOSED CIRCUIT TELEVISION SYSTEM

VERSION:	2.1
AUTHOR:	Neil Yates
IMPLEMENTED:	June 2017
REVIEW:	June 2018

CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

1.0 OVERVIEW

The Council has undertaken a Privacy Impact Assessment (PIA) of its existing CCTV system (Ribble Valley Borough Council Closed Circuit Television System).

The system was implemented in 2003, however the Council has undertaken this assessment to ensure continued compliance with legislation and adherence to good practice.

This document is based on the template incorporated into the Code of Practice by the Information Commissioner's Office (2015).

2.0 SCREENING QUESTIONS

These questions are intended to determine whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise.

QUESTION	ANSWER
1) Will the project involve the collection of new information about individuals?	Yes.
2) Will the project compel individuals to provide information about themselves?	Yes.
3) Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Only as a result of a 'Subject Access' request and subject to compliance with the Data Protection Act 1998.
4) Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used for?	No – it is a pre-existing system with no changes to be made.
5) Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	Yes – technology already in place.
6) Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	Action only to be taken by the Police.
7) Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	It may raise some privacy concerns or expectations but data is to be recorded and stored in a legal and safe way.
8) Will the project require you to contact individuals in ways that they may find intrusive?	No.
9) Has the research funder or data provider asked for the results of a Privacy Impact Assessment?	N/A

Table 2.1 Screening Questions

3.0 PRIVACY IMPACT ASSESSMENT FORM

STEP 01: IDENTIFY THE NEED FOR A PIA

The overall aim of the Council's CCTV system is to assist in the reduction of crime and the "fear of crime" by using overt and proactive public surveillance CCTV, providing a safer environment for the community across all areas covered by the system.

The specific purpose/objective of this system is to monitor public places within the areas covered in order to provide public assistance with the following:

- The prevention and detection of crime and provision of evidential material for judicial proceedings.
- To assist with operational policing by officers and community based staff in order to be more effective with Police and community safety resources.
- The maintenance of public order and community safety including the reduction of nuisance and vandalism and matters affecting citizens' quality of life.
- To enhance the feeling of safety, boost the economy and encourage greater use of the town centres and car parks.
- Assist the Local Authority in its enforcement and regulatory functions.
- The identification and management of traffic problems.
- The provision of appropriate information for town centre management.
- The training of CCTV operators, Police and Community staff.

Several of the screening questions were answered as 'yes' and therefore reiterated the need to complete a PIA.

STEP 02: DESCRIBE THE INFORMATION FLOWS

The collection, use and deletion of personal data can be described in the following way –

Data recorded from CCTV camera(s)
↓
Data stored on the recorders for a period of 31 days
↓
Data automatically "over-written" as part of process of erasure.

However, the Council also follows the requirements of the Criminal Procedures and Investigations Act 1996 which says that an investigator MUST retain material obtained in a criminal investigation, which may be relevant to the investigation.

This essentially means that when Police Officers or other investigators (DSS, Customers Officers etc) make a request to retain images, the CCTV staff will securely retain those images and deal with them according to agreed practices. Common law, as well as Section 19 of the Police and Criminal Evidence Act 1984 provides directions and powers in relation to items that have been seized by the Police.

The images are to be retained on the recording devices at the Control Room for no longer than 12 months or until any associated criminal or civil case has been completed.

An Image Review Log for the Authorities and Police requests will exist to record all "third party generated" reviews of digital images stored on the systems HDD. An example of the forms that will be part of this register is shown at Appendix D (Police Request) and Appendix E (Authorities Request).

An operator will complete the Image Review Log on EVERY OCCASION such access is gained to stored images. Access to stored images is also audited electronically within the systems HDD. This log sheet is self-explanatory and will contain all necessary information for all reviews and extracts where necessary. It will provide an easy access record of all review activity and provide a simple post-review for tracking and further work required from earlier reviews.

The logs will be retained securely within the CCTV Monitoring Room.

The System Manager will be responsible for the accuracy of the image review logs at all times. The log sheets will be kept for at least three years after the media has been destroyed.

Privacy risks are addressed by the following measures:

- Access to the control room restricted to authorised personnel only.
- Use CCTV operators who have been subjected to full security screening and be licensed as required by the Security Industry Authority (SIA) to meet the requirements of the Private Security Industry Act 2001.
- Record data on secure devices.
- Data to be stored and copies made as per the requirements set out above.

Formal consultation was undertaken prior to the installation of the system and no forthcoming changes are intended, it is therefore considered that no further consultation is required at this stage. However, dialogue with the Police is frequent and information is provided on the scheme signage that lists the Council's contact details, should members of the public wish to seek further information.

STEP 03: IDENTIFY THE PRIVACY AND RELATED RISKS			
The key privacy risks and associated compliance and corporate risks are listed as follows:			
PRIVACY ISSUE	**RISK TO INDIVIDUALS**	**COMPLIANCE RISK**	**ASSOCIATED ORGANISATION / CORPORATE RISK**
1) Storage of data.	If released could cause harm and distress to subjects and compromise any related Police investigation.	Could be accessed or hacked if not secure.	Could contravene legislation, such as the Data Protection Act (1998).
2) Release of data.	If released could cause harm and distress to subjects and compromise any related Police investigation.	Could be requested under 'Subject Access' request at which point the Council would lose control of the data.	Could contravene legislation, such as the Data Protection Act (1998).
3) Misuse of data.	If released could cause harm and distress to subjects and compromise any related Police investigation.	Person(s) accessing the data and using it for unauthorised means.	Could contravene legislation, such as the Data Protection Act (1998).

STEP 04: IDENTIFY PRIVACY SOLUTIONS			
The actions to be taken to reduce the risks and any future steps that are deemed necessary are listed as follows:			
RISK	**SOLUTION(S)**	**RESULT:** **Is the risk eliminated, reduced or accepted?**	**EVALUATION:** **Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?**
Could be accessed or hacked if not secure.	Data to be recorded on secure non-networked devices with appropriate security measures installed. Data to only be stored for timespans set out in manual and to comply with industry guidance.	Risk is reduced.	Measures carried out are as far as is reasonably practicable. Situation to be monitored any further technological developments or opportunities to be investigated and implemented if appropriate.
Could be requested under 'Subject Access' request at which point the Council would lose control of the data.	Require any person(s) who request footage to complete the appropriate form, detailing all relevant information relating to the request. When releasing footage, consider legal implications and requirements under legislation and only release footage that complies.	Risk is reduced.	Measures carried out are as far as is reasonably practicable.
Person(s) accessing the data and using it for unauthorised means.	Access to the control room is restricted to authorised personnel only. All CCTV operators have been subjected to full security screening and are licenced.	Risk is reduced.	Measures carried out are as far as is reasonably practicable.

STEP 05: SIGN OFF AND RECORD THE PIA OUTCOMES		
RISK	**APPROVED SOLUTION**	**APPROVED BY**
Could be accessed or hacked if not secure.	Data stored on secure devices.	Neil Yates, RVBC.
Could be requested under 'Subject Access' request at which point the Council would lose control of the data.	Require correct request forms to be completed and ensure compliance with legislation.	Neil Yates, RVBC.
Person(s) accessing the data and using it for unauthorised means.	Restrict access to authorised personnel only and only use licenced CCTV operators.	Neil Yates, RVBC/ Profile Security Ltd.
STEP 06: INTEGRATE THE PIA OUTCOMES BACK INTO THE PROJECT PLAN		
Data stored on secure devices.	Ongoing.	Neil Yates, RVBC.
Require correct request forms to be completed and ensure compliance with legislation.	Ongoing.	Neil Yates, RVBC.
Restrict access to authorised personnel only and only use licenced CCTV operators.	Ongoing.	Neil Yates, RVBC.
CONTACT POINT FOR FUTURE PRIVACY CONCERNS:		
Neil Yates, Engineering Services Manager, RVBC.		

Table 3.1 Privacy Impact Assessment Form

4.0 LINKING THE PIA TO THE DATA PROTECTION PRINCIPLES

The following questions are intended to identify where there is a risk that the project will fail to comply with the Data Protection Act 1998 or other relevant legislation, for example the Human Rights Act 1998.

PRINCIPLE 1	
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: *a) At least one of the conditions in Schedule 2 is met, and* b) *In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*	
Have you identified the purpose of the project?	Yes.
How will you tell individuals about the use of their personal data?	Scheme signage located throughout area of camera coverage.
Do you need to amend your privacy notices?	No.
Have you established which conditions for processing apply?	Yes.
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	Only process data that is approved unless refusal is overridden by legislation, i.e. criminal investigation.
If your organisation is subject to the Human Rights Act, you also need to consider: Will your actions interfere with the right to privacy under Article 8? Have you identified the social need and aims of the project? Are your actions are proportionate response to the social need?	 Only if the correct authorisation is not obtained when necessary. Yes. Yes.
PRINCIPLE 2	
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	
Does your project plan cover all of the purposes for processing personal data? Have you identified potential new purposes as the scope of the project expands?	Yes. Not currently.

PRINCIPLE 3	
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	
Is the quality of the information good enough for the purposes it is used?	Yes.
Which personal data could you not use, without compromising the needs of the project?	All footage is recorded with a view to being reviewed if deemed necessary. Any footage that is not required is automatically deleted from the system after 31 days.
PRINCIPLE 4	
Personal data shall be accurate and, where necessary, kept up to date.	
If you are procuring new software does it allow you to amend data where necessary?	Yes.
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	N/A.
PRINCIPLE 5	
Personal data processed for any purpose or purposes shall not be kept for longer than necessary for the purpose or those purposes.	
What retention periods are suitable for the personal data you will be processing? Are you procuring software that will allow you to delete information in line with your retention periods?	31 days for all footage and no longer than 12 months or until the completion of court proceedings for any footage used as evidence. Yes, software is already in place.
PRINCIPLE 6	
Personal data shall be processed in accordance with the rights of data subjects under this Act.	
Will the systems you are putting in place allow you to respond to subject access requests more easily?	Yes, a formal procedure is already in place and is considered appropriate.
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?	N/A.

PRINCIPLE 7	
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	
Do any new systems provide protection against the security risks you have identified?	Yes, systems are already in place.
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	To be compliant with the Code of Practice and Operational Procedures Manual. To be fully licenced by the Security Industry Authority (SIA). To shadow existing staff and be fully trained by the monitoring contractor as part of their induction, prior to taking on monitoring duties.
PRINCIPLE 8	
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	
Will the project require you to transfer data outside of the EEA?	No.
If you will be making transfers, how will you ensure that the data is adequately protected?	N/A.

Table 4.1 Linking the PIA to Data Protection Principles

REFERENCES

REPORTS

Information Commissioner's Office. (2015). *Conducting Privacy Impact Assessments Code of Practice*. Information Commissioner's Office.