Data Protection Impact Assessment (DPIA) - Full Assessment

Guidance for the Project Manager and Sponsor

Use the pre-screening template first. If that shows a high risk in processing the data then you must carry out this full DPIA. **Do not complete this form unless you have already completed the pre-screening and it shows high risk and the DPO as advised you to do a full DPIA.**

The Data Privacy Impact Assessment (DPIA) will enable you to systematically and thoroughly analyse how your project or system will affect the privacy of the people whose data you are dealing with and show how you will minimise the privacy risks. This template has been designed to incorporate the legal requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Conducting a DPIA is a legal requirement under the GDPR particularly if the proposed processing is using new technologies and poses a high-risk to people's data. Further information and guidance on the DPIA is also available on the ICO website here: ICO's PIA code of practice and the Article 29 Working Party here.

GOVERNANCE ARRANGEMENTS

This DPIA will be submitted to the Corporate Information Governance Group (CIGG) and the advice of the Data Protection Officer (DPO) will be sought as part of that process. You must keep the signed DPIA and all supporting documents with your project file for audit purposes.

1. **PROJECT SUMMARY**

Project Name	CCTV Privacy Intrusions	**Directorate and Service**	Supporting Communities, Security, CCTV
Project Sponsor and Position	CCTV Services Manager (SPOC)	**Project Manager and Position**	CCTV Services Manager (SPOC)
Project Start Date **Project End Date**	Dec 2020 TBC 2021	**Project Go Live Date (anticipated/planned)**	TBC 2021

Third parties involved/associated with the Project:	Tyco Integrated Services (Organisations CCTV contractor)	**Does this DPIA cover multiple projects?**	No

High Level description of the Project:

- *Explain what this project is in plain language. For example: "We would like to share data with a third party so that they can carry out research into how to improve people's access to benefits."]*
- *Attach the pre-screen DPIA. The conclusion to that will explain why it is necessary to carry out this DPIA.*

The organisation is running two CCTV systems and associated assets. It has identified a significant number of CCTV cameras with a potential to cause privacy intrusion. This is due to where many 'historic' cameras are installed/positioned pre Home Office Surveillance Camera Commissioner Code of Practice. Majority of these potential privacy intrusions are on housing estates with a much smaller volume on Highway cameras.

Residents who could possibly be affected may feel the camera can see straight inside their properties, with resultant privacy concerns. Whilst the positioning of the camera appears this to be the case, this only relates to a few cameras with the vast majority of cameras only being able to do so, in the event a CCTV Operator miss-used a camera and zoomed into windows of a property.

This document aims to:

1. Outline organisation's approach in managing potential privacy intrusions with the archaic Housing CCTV system. System has inability to apply privacy masking on each camera as required due to inadequate technologies
2. Outline organisation's approach in managing potential privacy intrusions with Highway CCTV system. System has ability to apply privacy masking on each camera as required

2. DESCRIPTION OF THE PROJECT

Include here a plain English description of:

- *the Project (set the context so that it is clear what you want to do)*

There are c900 Housing Cameras, and the majority are fed off an antiquated, obsolete CCTV system with inability to apply privacy masking on each camera where potential intrusion of privacy may apply. The vast majority of the c900 housing cameras have some form of privacy intrusion. A folder already exists of all identified privacy intrusions.

In Spring 2021 Housing CCTV upgrade project commences. It is set to take approximately 3 years to completion. The Project entails each camera is assessed to see if fit for purpose, positioned in best location to record and monitor, remove or upgraded to latest technology, allowing ability to eliminate/reduce existing or future levels of privacy intrusion.

Housing Cameras: until upgrade project, this document is to acknowledge the significant level of intrusions and present options.

Option 1: Reactive Approach

Currently where a complaint is received regarding privacy intrusion, the Organisation's initial response will be to reposition the camera in such a way, complainant is reassured and satisfied without incurring additional intrusion elsewhere.

Where reposition may not be possible due to technology or further privacy intrusions understood the camera will be removed.

A replacement camera will be reinstalled as part of the housing CCTV upgrade project when that location is being upgraded, in same location on condition there is a pressing need and legitimate aim for installation. This means that a reactive approach is planned, responding to individual complaints.

However this approach is sub-optimal, as it does not comply with the GDPR requirements of privacy by default and design, and leaves reliance on data subjects to complain, rather than the council dealing with issues proactively as is required by data protection legislation. Individual data subjects may not be aware of the privacy intrusion, and it is not appropriate to leave the onus on them. The onus is on the council to assess the risk and mitigations.

Option 2: Pro-active Approach

Each camera's privacy intrusion has been completed, with illustrated screen shots displaying camera's field of view of intrusion.

As these cameras/system do not have technical ability for privacy masking, they would need to be removed requiring a project team of CCTV engineers and a budget, neither of which are held by the CCTV team. There will be limited or no technical issues associated with removing a lot of these antiquated assets which may result in a significant number becoming non-operational. However, as these assets are antiquated becoming non-operational is not for consideration.

To remove cameras before the planned upgrade is unlikely to cause problems with the upgrade programme however, would result in limited or no CCTV coverage across the borough housing land.

This then impacts on **(a)** resident/community perception of safety and security and **(b)** tenant and leaseholder CCTV charges very limited or nil. Leaves housing land/majority of them without camera cover potentially up to 3 years. **(c)** This would leave areas vulnerable to crime, anti-social behaviour, safety and security - issues the cameras are designed to prevent and detect.

Until upgrade - cameras would be recording in the background and **not** displayed on large wall monitors within control room. CCTV Operators would only actively look at a specific camera in the event of a real time incident or retrospectively review recorded footage, within the last 31 days (recorded data automatically held for this time) in relation to an incident. Should intrusion of privacy be identified on recorded footage, footage would need to be escalated to CCTV Manager in the first instance, Head of Security or CCTV Corporate Owner to authorise/decline release/processing of data. This would become part of the Service Operational Procedure (SOP)

The practice of declining footage already exists where Freedom of Information (FOI) and Subject Access Requests (SAR) are received. Where living identifiable persons maybe recorded, the request is usually declined and CCTV Operator writes an incident report of sequence of events as seen on CCTV footage in relation to incident as an acceptable alternative.

Option 3: Swap Out Approach

Remove all affected cameras (vast majority) before housing upgrade project and install new cameras that would be used as part of the upgrade. However, new cameras for upgrade require a resilient new CCTV designated network (infrastructure) which needs to be designed and built prior to any new cameras installed which sits on the network. Upgrade project award is likely to complete end of December 2020 and therefore timelines required coincides with this option, in the most part.

Option 4 Combined approach

During the upgrade period, leave all cameras in situ and replace as upgrade programme. Deal reactively with complaints as they are received in as Option 1 but combine that with proactive actions for the highest risk cameras: all the **steps above for lower risk cameras would be followed, and also** these cameras would be prioritised on the replacement programme as far as technically possible.
This would ensure the highest risk cameras were dealt with quickly, steps put in place in the interim, and complaints dealt with quickly and effectively.

Option 4 is recommended as a balance of lowering data protection risks whilst ensuring technical limitations are not exceeded

Highway cameras commencing February 2021 a roll out programme will commence in order to apply privacy masking to identified intrusions.

An electronic folder already exists of all identified privacy intrusions which will be updated to show before and after image(s) once privacy masking applied. Each camera's privacy intrusion has been completed, with illustrated screen shots displaying camera's field of view of intrusion. This brings compliance to: **(1)** CCTV service delivery, **(2)** GDPR and **(3)** SCC (Surveillance Camera Commissioner) Code of Practice

RDC (Rapid Deployable Cameras) newly installed on various locations pertaining to monitoring housing land assets is the latest technology of cameras, fit for both current and future purpose. Technology has ability to apply privacy masking and as such has been applied where required.

Below examples of privacy intrusion on Housing and Highway cameras

Housing CCTV

FIG 1. Demonstrates a recent **RDC** installation in November 2020 on Housing land at Munster Square, Marlston Block. Installation as a result of safeguarding with immediate threat to life, Police involvement and Camden legal approving after querying possible RIPA implications.

- Photo on **left** displays 3 properties (doors/windows). The property of interest is the middle property (door/windows).
- Photo on left shows camera view with potential intrusion on two other properties (left and right of centre property).
- Photo on right show privacy masking applied ensuring there is no intrusion to properties either side of centre property.



Highway Camera 1 – examples of privacy intrusions multiple locations from one camera. This would be part of the privacy masking programme to masked out windows





Examples of privacy intrusions multiple locations from one camera. This would be part of the privacy masking within the Housing CCTV upgrade to masked out windows



- *what will be done with the data (the processing activities)*

Any data recorded automatically stored for 31 days on CCTV server, thereafter automatically erased.

Where data has been requested, data manually extracted from CCTV server (By CCTV Operator) based on date, time and nature of

incident. This is then held in CCTV system evidence locker for as long as necessary to meet purpose it has been saved – generally applies to Police and Council Officers. Then burnt to encrypt DVD or uploaded to TEAMS if internal. Data usually collected within 10 working days, manually erased (By CCTV Operator) from evidence locker thereafter and full audit logged for 12 months.

CCTV system evidences every action an individual CCTV Operator conducts, from the moment of logging into system via individual login and password to moment of log off. Where a complaint of intrusion may be received, system evidences which CCTV Operator used an individual camera based on complaint details i.e. camera number, location, date, time.

- *the reasons why you need to process the data (the purpose)*

  Evidential purposes - Usually for crime, road accident, subject access request, Anti-social behaviour, personal injury, building insurance etc. for a specified incident i.e. for crime/insurance claim, police,

- *the benefits that this project will provide*
  Residents reassured organisation managing risk - Risk clearly identified and documented

  - To **reassure** residents cameras which appear to look into properties are not. That for all CCTV Operators operating the system, their actions are fully auditable for accountability. In line with CCTV policy, where miss-use of a camera(s) is evidenced then disciplinary actions will be applied. All Operators are Security Industry Licenced (SIA) and trained with knowledge and skills to operate camera(s) to be non-intrusive where possible

  - To **evidence** management of potential camera privacy intrusion, has a disciplinary process, operator usage identifiable on system, camera installed where at the time there was a need, annual camera reviews identifying each camera still meets the objective set out to achieve i.e. reduce/deter crime and Anti-Social Behaviour (ASB), promote a feeling of safety within community. To apply privacy masking screens to each area of camera intrusion i.e. property windows where technology allows

  - To **remove** cameras where no other alternative can be reached. A camera will be removed should a complaint be received and camera cannot be relocated avoiding any intrusion and or masked

- *how the data will be processed (for example, who will carry out the processing and will they use software or other devices to do it)*

Operating and processing of any CCTV data will be carried out by (SIA) security industry authority licenced CCTV Operators, in operating cameras, how General Data Protection Regulation (GDPR) affects what they do where intrusion of privacy is concerned and CCTV local policy and procedures i.e. when moving a camera pan downwards to avoid moving across windows, home position of cameras not zoomed in and directed towards a window. Recorded data only extracted and downloaded onto encrypted DVD in the event a written request is made. Request where required is authorised for release with witness statements. Data collected in person or point to point courier or electronically via TEAMS if internal.

- *how will the data be stored?*

- Complaint process – any complaint received on privacy intrusion will be logged and stored in line with organisations complaints policy/procedure
- Subject Access Requests (SAR) - any SAR received on privacy intrusion will be logged and stored in line with organisations complaints policy/procedure
- CCTV system – stored on CCTV secured system. System actions auditable for every action.

- *where have you obtained the data from?*

Data obtained from central CCTV system which already has its own DPIA sign off and can be appended to this as required.

- *How long will you be processing the data for and how often? For example, once a week for six months.*

  Data only used if legitimate request with an approximate turnaround from point of request to releasing data 14 working days. Data usually current data used within 31 days

- *What is the volume of the data? For example, 150 records of service users.*

  Request average at 150 per month. Approximately 30% of requests for data received is a negative of some kind.

Types of personal data to be processed and data flow map(s):

Personal data:

List the types of data that you intend to process and the types of data subject (for example, names, addresses of residents, service users etc):

- *Refer to this guidance to assess what is personal data:* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

Special category data:

List the types of special category data and the types of data subject:

- *Refer to this guidance to assess what is special category data:* **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/**
- *Any criminal convictions data?*

Special category data is not the intended capture, but may be incidentally captured through footage.

Data Flows:

- *You may find it useful to use a flowchart, which you can attach at Annex A.*
- *The flowchart should show, for example: Data entry and exit points, location, user categories, data subject categories*

3 DATA PROTECTION PRINCIPLES

This section demonstrates how the project meets the data protection principles.

- How will you make sure that you only process the data that is necessary and proportionate for the purpose of the project, and no more than is necessary?

Currently archaic CCTV system is not able to apply privacy masks to majority of cameras due to old technologies. Images recorded has potential to record views of windows/doors/balconies.

Part of licensing and training ensures Operators trained not to zoom into windows or leave cameras directed to/zoomed into windows, gardens, balconies or doors.

Due to trained Operator requirements any images being tracked/recorded in real-time, where an Operator is operating the camera, should not be zooming into windows/balconies/doors.

However, dependant on nature of incident being tracked/recorded in real-time windows/balconies/doors may be subject to camera being focussed on.

- If the data was originally collected for one purpose and you intend to use it for another purpose, explain how you will inform the data subjects.

  Not applicable

- How will you make sure that the data is kept accurate and up to date?
- How long will you keep the data for and how will you destroy it at the end of the retention period?

The remaining parts are covered in the overarching CCTV DPIA

- Have you cleared the information security arrangements with the Information Security Manager? YES/ NO
- **Record the Information Security manager's comments here:**

This is covered in the overarching DPIA

4 BASIS OF PROCESSING

1. Which legal basis in Article 6 are you relying on? See this guide to help you identify the legal basis https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

   (e) Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

2. If you think you need to rely on legitimate interests then ask the Information and Records Management Team for advice.
3. If you are processing special category data, you will also need a legal basis under Article 9 to process this. See this guide to help you identify the legal basis **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/**

   Not applicable

4. If you are processing criminal convictions data or data for law enforcement reasons then you should speak to the Legal team as you need an additional legal basis to do this.

   Not applicable

Basis for processing under Art 6 (and Art 9 if special category data):

(e) Public task: the processing is necessary to perform a task in the public interest for official functions, and the task or function has a clear basis in law.

5 DISCLOSURES OF DATA

- Will you be transferring/ sharing/giving this data to a data processor or a sub-processor? **~~YES~~/ NO**

  No

- Tick here to agree that you will be entering into a data processing agreement with them **[ ]**

  Not applicable

- Will you be sharing data with any other third party? **YES/** ~~NO~~

  Yes

- List the third parties that you propose to share with:

  Law enforcement Agencies, Insurance Companies, Subject Access Requests

- Tick here to agree that you will be entering into a data sharing agreement with the third parties **[✓]** Data sharing agreements are in place/will be in place for all routine sharing. Ad hoc sharing such as with non-local police, or data subjects under SAR do not require DSAs.

6 TRANSFERS OF DATA OUTSIDE OF THE EEA

Will any personal data be processed outside of the UK? ~~YES~~/NO
If yes will it be processed out of the EEA? N/A
See a list of countries here: https://www.gov.uk/eu-eea

If your answer is yes, you must consult the DPO straight away, and see the guidance here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

If there WILL be a transfer out of EEA enter comments of the data protection advisor:

To contain comments detailing the safeguards that need to be put in place.

Not applicable

7. DATA SUBJECT RIGHTS AND COMPLIANCE WITH CORPORATE POLICIES

Information in Camden contains the Council's policies and procedures on data protection compliance, including how to respond to requests from people to enforce their rights under data protection law.

- You must comply with the requirements in Information in Camden. Tick here to agree that you will be complying with IIC on Data Subject Rights **[✓]** If there is a reason why you cannot do this, please explain why here:

Not applicable

8. CONSULTATION WITH INTERESTED PARTIES

Is one of the outcomes of your project going to make a change which will have a direct effect on data subjects? For example: introducing CCTV into a library? If so, contact the Information and Records Management Team for advice at dpa@camden.gov.uk about whether you need to consult with stakeholders.

Record the comments of the data protection adviser here:

To include advice on whether consultation is necessary and the steps to take. Consultation not necessary, assets already installed. A consultation has recently gone to all housing land residents regarding Housing CCTV upgrade project commencing spring 2021. This project entails latest technology upgrades for cameras and systems with ability of privacy masking - therefore meeting objective of minimal/eliminating intrusion

9. RISK ASSESSMENT AND MITIGATION

Risk is a combination of **impact**- how bad the effect of the risk would be- and **probability** – the likelihood of the risk happening**.** Risk is assessed from the perspective of the data subject (as opposed to risk to the Council) and what the impact could be on them as a result of the proposed data processing. For each of the risks you identify:

1. think about how likely they are to occur and categorise them according to **Table 1 in the appendix (e.g., rare, unlikely etc)**.

2. Then consider the impact each risk will have and categorise them according to **Table 2 in the appendix (e.g., minor, moderate etc)**.

3. Then look at **Table 3** and see the risk level. Where the level says mitigations are needed, think about what these will be and how they will reduce the risk level down.

4. Enter the details in the grid below

There is more information on the council's approach to risk here
https://lbcamden.sharepoint.com/sites/intranet/finance/Pages/Risk_Management.aspx

Risk 1 *[include as many rows as necessary to identify each risk individually]*	**Risk Level Before any Mitigations**	**Risk Level After Mitigations**
Source of risk: Highways cameras where manual positioning by operators could allow for privacy intrusion Of those that are affected these have been assessed into 2 risk categories: Higher level of privacy intrusion and lower level intrusion 215 Highway Cameras of which **211 have intrusion/98%** of which 14 (7%) cameras have a lower level of intrusion. 7 of these cameras we are unable to connect to at the time of writing this document due to technical issues and as such will include as having privacy intrusion 4 of these cameras have no privacy intrusion = 1.9%	**Medium/high risk**	**Medium risk**

Potential impact on individuals: Intrusion of privacy within private property, distress, embarrassment, lack of control and agency, lack of privacy **Any compliance or corporate risks?** (refer to the council's approach to risk here https://lbcamden.sharepoint.com/sites/intranet/finance/Pages/Risk_Management.aspx if you need to) Reputational negative impact, lack of GDPR compliance leading to enforcement action and possible financial penalties, damages actions from affected people, breach of Home Surveillance Camera Commissioner guidelines for local authorities **Where mitigations are required what these are?** Commencing February 2021 (currently seeking to bring roll out forward to January 2021) a roll out programme will commence in order to apply privacy masking to the identified intrusions. This will eliminate risks for these cameras. In the interim due to the nature and positioning of these cameras, cameras cannot be taken out of operation until the privacy masking is implemented. Cameras will remain in place with the following safeguards: 1. All Operators are and trained with knowledge and skills to operate camera(s) to be non-intrusive where possible 2. Operators are all Security Industry Licenced (SIA). 3. All CCTV Operators actions are fully auditable for accountability 4. In line with CCTV policy, where miss-use of a camera(s) is evidenced then disciplinary actions will be applied		
Risk 2		
Source of risk: Housing cameras where manual positioning by operators could allow for privacy intrusion	**High Risk**	

Of those that are affected these have been assessed into 2 risk categories: Higher level of privacy intrusion and lower level intrusion 960 housing cameras of which **698 have intrusion/73%** of which 10 (1.4%) cameras have a lower level of intrusion. 563 of these cameras we are unable to connect to at the time of writing this document due to technical issues and as such will include as having privacy intrusion 262 of these cameras have no privacy intrusion = 27% **Potential impact on individuals:** Intrusion of privacy within private property, distress, embarrassment, lack of control and agency, lack of privacy **Any compliance or corporate risks?** (refer to the council's approach to risk here https://lbcamden.sharepoint.com/sites/intranet/finance/Pages/Risk_Management.aspx if you need to) Reputational negative impact, lack of GDPR compliance leading to enforcement action and possible financial penalties, damages actions from affected people **Where mitigations are required what these are?** Commencing Spring 2021 there will be a Housing CCTV upgrade project, which will take approximately 3 years to completion. The project entails each camera being assessed to see if it is fit for purpose, positioned in best location to record and monitor, remove or upgraded to latest technology, allowing ability to eliminate/reduce existing or future levels of privacy intrusion. At the end of this programme all risks will have been removed. **In the interim**: there is a list of all affected cameras - not all housing cameras are affected. Of those that are affected these have been assessed into 2 risk categories: Higher level of privacy intrusion and lower level intrusion.		**End of replacement programme low risk throughout** **During replacement programme risk varies according to option followed**

Where the privacy risks are not high cameras will remain in place with the following safeguards: **1.** Cameras would be recording in the background and **not** displayed on large wall monitors within control room. **2.** CCTV Operators would only actively look at a specific camera in the event of conducting daily camera checks to ensure camera operational, a real time incident or retrospectively review recorded footage, within the last 31 days (recorded data automatically held for this time) in relation to an incident. **3.** All Operators are and trained with knowledge and skills to operate camera(s) to be non-intrusive where possible **4.** Operators are all Security Industry Licenced (SIA). **5.** All CCTV Operators actions are fully auditable for accountability as system tracks usage **6.** In line with CCTV policy, where miss-use of a camera(s) is evidenced then disciplinary actions will be applied **7.** Operators will have special instructions about the risks of these cameras **8.** These cameras will be prioritised in the replacement programme **Where the privacy risks are high** There are four options: (with the inclusion of points 5 to 12 above where applicable) **Option 1: Reactive Approach** Where a complaint is received regarding privacy intrusion reposition the camera in such a way to reduce intrusion, **and also follow the steps above for lower risk cameras**. Where reposition may not be possible due to technology or further privacy intrusions the camera will be removed. A replacement camera will be reinstalled as part of the housing CCTV upgrade project when that location is being upgraded, in same location on condition there is a pressing need and legitimate aim for installation. This means that a reactive approach is planned, responding to individual complaints.		**During replacement programme:** **Lower risk cameras: medium/low risk** **During replacement programme:** **Higher risk cameras:** **Option 1: Medium/high risk**

However this approach is sub-optimal, as it does not comply with the GDPR requirements of privacy by default and design, and leaves reliance on data subjects to complain, rather than the council dealing with issues proactively as is required by data protection legislation. Individual data subjects may not be aware of the privacy intrusion, and it is not appropriate to leave the onus on them. The onus is on the council to assess the risk and mitigations. **Option 2: Pro-active Approach** As these cameras/systems do not have technical ability for privacy masking, they would need to be proactively removed before the upgrade programme. Removal would remove the privacy risks however has other knock on negative effects. It would require a project team of CCTV engineers and a budget, neither of which are held by the CCTV team. There will be limited or no technical issues associated with removing a lot of these antiquated assets which may result in a significant number becoming non-operational. However, as these assets are antiquated becoming non-operational is not for consideration. To remove cameras before the planned upgrade is unlikely to cause problems with the upgrade programme. **However, it would result in limited or no CCTV coverage across the borough housing land.** This then impacts on **(a)** resident/community perception of safety and security and **(b)** tenant and leaseholder CCTV charges very limited or nil. Leaves housing land/majority of them without camera cover potentially up to 3 years. **(c)** This would leave areas vulnerable to crime, anti-social behaviour, safety and security - issues the cameras are designed to prevent and detect. **Option 2 is the best option for privacy but perhaps not the most practical option for other considerations.** **Option 3: Swap Out Approach** Remove all affected cameras (vast majority) before housing upgrade project and install new cameras that would be used as part of the upgrade. However, new cameras for upgrade require a resilient new CCTV designated network (infrastructure) which needs to be designed and built prior to any new		**During replacement programme:** **Option 2:** **Low risk privacy but high risk public safety** **Not viable option**

cameras installed which sits on the network. Therefore this is not practical as cannot be undertaken swiftly. **Option 4 Combined approach** During the upgrade period, leave all cameras in situ and replace as upgrade programme. Deal reactively with complaints as they are received in as Option 1 but combine that with proactive actions for the highest risk cameras: all the **steps above for lower risk cameras would be followed, and also** these cameras would be prioritised on the replacement programme as far as technically possible. This would ensure the highest risk cameras were dealt with quickly, steps put in place in the interim, and complaints dealt with quickly and effectively. **Option 4 is recommended as a balance of lowering data protection risks whilst ensuring technical limitations are not exceeded**		**Medium risk during programme, low risk at completion**

10. OVERALL RISK RATING FOR THE PROJECT AS A WHOLE ONCE THE MITIGATING MEASURES HAVE BEEN PUT IN PLACE:

When housing replacement programme completed: **LOW**	**During replacement programme:** **MODERATE if option 4 followed**	**MEDIUM/ HIGH**	**HIGH**

ANNEX A: DATA FLOW MAPS – n/a see main CCTV DPIA

ANNEX B Risk Assessment Tables

Table 1 Likelihood of Risk Occurring

Rare	One-off failure
Unlikely	Possible that it may reoccur but not likely
Possible	Might happen or reoccur on a semi-regular basis (no more than once a quarter)
Likely	Will reoccur on a regular basis, pointing to some failure in controls
Almost Certain	Wilful act, systemic failure in controls

Table 2 Impact of Risk if it occurs

Negligible	No personal data involved, or risk won't have any impact.
Minor	• Short-term, minimal embarrassment to an individual • Would involve small amounts of sensitive personal data about an individual • Minimal disruption or inconvenience in service delivery to an individual (e.g. an individual has to re-submit an address or re-register for a service)
Moderate	*More than a minimal amount of sensitive personal data is involved at this level* • Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family) • The potential of a financial loss for individuals concerned • Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual (e.g. availability to a set of personal information is lost, requiring resubmission of identity evidence before services

Major	Significant amount of HR, or resident personal, and / or sensitive data released outside the organisation leading to significant actual or potential detriment (including emotional distress as well as both physical and financial damage) and / or safeguarding concerns
Catastrophic	Catastrophic amount of HR or service user personal and or sensitive data released outside the organisation leading to proven detriment and / or high-risk safeguarding concerns. Data subjects encounter significant or irreversible consequences which they may not overcome (e.g. an illegitimate access to data leading to a threat on the life of the data subjects, layoff, a financial jeopardy)

Risk Assessment: Table 3

	Score:	**PROBABILITY**				
		Rare	Unlikely	Possible	Likely	Almost Certain
IMPACT	Catastrophic	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Negligible	1	2	3	4	5

Level of risk	
1-3 Low Risk	Acceptable risk No further action or additional controls required Risk at this level should be monitored and reassessed at appropriate intervals
4-6 Moderate Risk	A risk at this level may be acceptable, if so no further action or additional controls required If not acceptable, existing controls should be monitored or adjusted
8-12 Medium / High Risk	Not normally acceptable Efforts should be made to reduce the risk, provided this is not disproportionate Determine the need for improved control measures
15-25 High Risk	Unacceptable Immediate action must be taken to manage the risk A number of control measures may be required

Annex C:
Any DPO Advice or comments not included above

There are clearly a number of privacy issues raised by the use of our CCTV cameras. These have come about as a result of the age of the infrastructure, changing technical capabilities and expectations regarding privacy and the piecemeal way in which the estate has been created. While recognising the privacy issues and not discounting them this is a clear plan to tackle them while recognising the continued benefit of leaving the equipment in situ. We should however review the position again in 12 months.

20TH July 2021 post script

I was made aware of the funding issue and its resolution. Noted that the plan is back albeit slightly delayed.

Andrew Maughan - DPO