BRADFIELD PARISH COUNCIL

Clerk to the Council: Mrs Marie Snell
Bradfield Village Hall.The Street, Bradfield, Essex CO11 2UU Tel: 07851 760264
E-mail: clerk@bradfieldparishcouncil.org.uk

CCTV Data Privacy Impact Assessment (DPIA) and Risk Assessment

This document sets out the council's DPIA process and risk assessment. It follows the process set out in our Information Commissioners Office (ICO) DPIA guidance.

This document will be reviewed annually, and also when starting a major project involving the use of personal data or if we are making a significant change to an existing process.

A copy of this document is available on our website or by contacting the Parish Clerk (details below).

Submitting controller details

Name of controller	Bradfield Parish Council
Subject/title of DPO	Parish Council Clerk
Name of controller contact (delete as appropriate)	Marie Snell (Clerk) Email:clerk@bradfieldparishcouncil.org.uk Tele: 07851 760264

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The parish council has identified that the access road and council car park adjacent to the village hall, plus the village hall surrounds (VH by the council, land owned by Bradfield Allotment and Recreation Ground Charity) is subject to the following antisocial behaviour: 1. Unauthorised dumping of material near to the recycling containers 2. Possible drug-related activity 3. Unauthorised parking due to a security barrier breach By installing CCTV, the aim is to provide a deterrent and also capture images in order to assist the police should further action be necessary.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
Data will be collected by cameras attached to the village hall and will focus on the car park. The cameras will be linked to a recorder, which will be installed in a lockable security box and located within a locked office at the village hall. Access to the office and recorder will be restricted to council authorised persons. The recorder will store data for a period of 31 days, after which it will be destroyed. Stored data can be securely accessed remotely via the internet, by the authorised users. Access to the system and any action taken will be logged by the authorised users. Requests to share data will be considered from the police if appropriate or if formally requested by a member of the public through a Subject Access Request (SAR).

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
The data will record any members of the public using the access road, car park adjacent to the village hall and the village hall surrounds. The cameras are not trained upon any housing and will be operating on a 24/7 basis. The council has considered the criteria regarding Special Category Data and is of the view that the collection of data for the purposes outlined above does not raise any issues. The council will collect data only for the period as stated in Step 2 (i.e. 31 days) after which it will be destroyed, unless it is retained specifically within the context of an investigation and possible prosecution.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
The parish councillors are elected by those within the parish and are themselves residents. The area covered within this DPIA is used by the local community and others from further afield. The council publishes a data privacy notice and will put in place a CCTV policy plus this DPIA on its website, which will clarify an individual's right to request any of their personal data that the council may hold. The council is not aware of any previous concerns regarding the use of CCTV.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
The council would like to reduce antisocial behaviour. The aim is that the installation of CCTV will provide a deterrent and send a message to those individuals that their behaviour is unacceptable. The benefit for the council is that the use of CCTV will enable more control over this public space and will provide reassurance to members of the community.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
The local community have the opportunity to raise concerns and discuss the issue through council meetings, by contacting parish councillors or the parish clerk directly or at a 'Meet Your Councillor' session. They have been updated via council meeting minutes (available on our website and village noticeboards), social media, and the village magazine. The council has sought support from the National Association of Local Councils and also canvassed other local councils who employ CCTV. As part of the fact finding the council has spoken to suitably qualified installers of CCTV systems.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
The council has the power to act under the Local Government and Rating Act 1997 s. 31 which states: *Crime prevention.* *(1) A parish council or community council may, for the detection or prevention of crime in their area—* *(a) install and maintain any equipment,* *(b) establish and maintain any scheme, or* *(c) assist others to install and maintain any equipment or to establish and maintain any scheme.* The council has assessed this and feels that this measure is the next step in reducing antisocial behaviour. The Data Privacy Notice has been reviewed and updated where appropriate and a CCTV Policy has been created, both of which have been approved by full council.

Individuals will be made aware that they have the right to request information on their personal data held by the council by contacting the Parish Clerk.
Authorised users of the CCTV system will receive training in the secure use of the equipment and also the maintenance of a log which details any action taken.
The equipment will be maintained through an agreement with an approved contractor.
International Transfers- any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, Possible Probable	Minimal, Significant Severe	Low Medium High
1. Recording device in the village hall accessed by unauthorised persons-release of personal data	Possible	Significant	Medium
2. Online hacking-release of personal data	Possible	Significant	Medium
3. Lack of maintenance of equipment results in poor or no coverage when required	Possible	Significant	Low
4. Equipment vandalised-additional cost to community	Possible	Significant	Medium
5. Data Privacy Notice, CCTV policy and procedures not reviewed and updated. Leaves council open to litigation.	Remote	Severe	Low
6. Unauthorised requests for data permitted	Possible	Significant	Low
7. Public unaware of CCTV in operation. Leaves council open to litigation	Possible	Severe	Low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk (see Step 5)	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated Reduced Accepted	Low Medium High	Yes/no
1.	Recording device kept in secure container & located in a locked office at village hall	Reduced	Low	Yes
2.	ICO guidelines for protecting data (CCTV Policy & Procedure)	Reduced	Medium	Yes
3.	Equipment serviced and repaired under a maintenance agreement with approved contractor. Checks by approved system users	Reduced	Low	Yes
4.	Equipment insured	Reduced	Medium	Yes
5.	Policies and procedures reviewed regularly. Training records kept for authorised users	Reduced	Low	Yes
6.	Clear guidelines in place to identify the validity of request. Single contact for requests i.e. Clerk Record kept of any requests for information.	Reduced	Low	Yes

7.	Privacy Notice and CCTV Policy made available through council website and social media. Information notices installed within identified areas	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:	Full Council meeting dated 5th March 2024. Minute 188/23a	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Full Council meeting dated 5th March 2024. Minute 188/23a	If accepting any residual high risk, consult the ICO before going ahead
Data Protection Officer (DPO) advice provided:	N/A	See below
Extract from NALC paper 'A GDPR Toolkit for local councils-August 2018 v 3', section 26.1 states: *'Under the DPA 2018, local councils (and parish councils and parish meetings) are excluded from the definition of 'public authority or body'. This means that local councils do not automatically have to have a DPO unless you process personal data for regular and systematic monitoring of data subjects on a large scale, or process sensitive personal data on a large scale. If either of these apply, you will need to appoint a DPO.'*		
DPO advice accepted or overruled by:	N/A	
Comments: N/A		
Consultation responses reviewed by:	See Step 3	If your decision departs from individuals' views, you must explain your reasons
Comments:		