THE IVERS PARISH COUNCIL

45B High Street, Iver, Buckinghamshire, SL0 9ND
www.iversparishcouncil.gov.uk

Agenda Item	**CCTV System Upgrade**
Meeting Date	**Full Council – 16 December 2024**
Report Title	**Iver and Iver Heath Recreation Ground Additional CCTV Coverage**
Recommendation/s	**1. To install 3 additional cameras at the Jubilee Pavilion.** **2. To install 1 additional camera on the Iver Recreation Ground Workshop.** **3. To install 1 additional camera to the Iver Heath Recreation Ground car park pole.** **4. To install 1 additional camera at the Parish Council office to cover the front door.** **5. To purchase additional hard drive capacity to retain recordings for 30 days.**
Appendices to Report	**1. Data Protection Impact Assessment**
Prepared By	**Nicole McCaig – Deputy Clerk**

Detailed Information

Project History

The Council's Open Spaces & Highways and Facilities & Events (F&E) Committees considered the requirement for an upgrade to the CCTV systems to include additional coverage of the open spaces at Iver and Iver Heath Recreation Grounds.

The F&E Committee reviewed and updated the Council's CCTV policy on 4 September 2024.

Officers further considered the need for an additional camera at the Council offices to protect the personal safety of staff working in the reception area which is freely open to the public during the working day.

Data Protection

In November 2024, the Council's Data Protection Officer (DPO), Satswana Ltd, assisted officers to complete a Data Protection Impact Assessment (DPIA), as required by the Data Protection Act 2018. A DPIA is required as the Council is proposing to update a key system that will affect how the Council records CCTV footage of publicly accessible open spaces.

The DPIA identified the privacy risks and potential impact on individuals associated with upgrading the CCTV system to include additional cameras. The DPO found no high risks

associated with the upgrade and therefore there is no need to contact the Information Commissioner's Office before commencement of the upgrade.

Considering this, officers are recommending that the installation of additional cameras can proceed.

The benefits are as follows:

- The Council's owned and managed land will be included in the CCTV coverage.
- CCTV recordings of suspected anti-social behaviour will be possible and can be provided to the police when requested.

The installation of additional cameras and hard drives will be completed by the Council's existing CCTV provider.

Key Implications	
Financial	2 x additional hard drives: £295 Supply and installation of 6 x cameras: £2,910 Total CCTV budget currently available: £2,225 CCTV Budget overspend: £980
Legislative and Policy	Data Protection Act 2018 (incorporating the General Data Protection Regulation (GDPR)) The Protection of Freedoms Act 2012 The Surveillance Camera Code of Practice (2022) The Council's CCTV Policy and CCTV Privacy Notice
Equality Assessment	The CCTV is possible of picking up special category data including race, ethnic origin, health of an individual and physical characteristics.
Net Zero	There are no Net Zero implications

satswana

Data Protection Impact Assessments (DPIA)

What you need to know
This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, which should be read alongside it, and the criteria for an acceptable DPIA set out in European guidelines on DPIAs. You should start filling out the template at the start of any major project involving the use of personal data or if you are making a significant change to an existing process. Introduction

This procedure sets out the principles by which The Ivers Parish Council (now called 'Council'), who is the 'Data Controller,' will develop, manage, and review the management of Data Protection Impact Assessments (DPIA).

The Information Commissioner's Office defines a DPIA as:

'a process that helps assess privacy risks to individuals when collecting, using, and disclosing information. DPIA helps identify privacy risks, foresee problems and bring forward solutions.'

A DPIA is a tool that allows for proper planning to effectively implement new or changed systems while assuring the confidentiality, security, and integrity of Personal Confidential Data or Business sensitive data.

Scope
This procedure applies to all staff and visitors all processes that include a new or changed use of Personal Confidential Data or Business sensitive data in any format.

Typical examples are:

- introduction of a new paper or electronic information system to collect and hold personal/business sensitive data;
- The introduction of a new service or a change to an existing process may impact an existing information system.
- updating or revising a key system that might alter how the Council uses, monitors, and reports personal/business-sensitive information.
- replacement of an existing data system with new software, changes to an existing system where additional personal/business sensitive data will be collected
- proposal to collect personal data from a new source or for a new activity
- plans to outsource business processes involving storing and processing personal/business-sensitive data
- plans to transfer services from one provider to another that include the transfer of information assets
- any change to or introduction of new data-sharing agreements

Determine
Members of staff should establish and document:

- The purpose of processing the data
- Who are the Data Controllers (sole, joint or in common) and Data Processors (see below for details)
- The legal basis for sharing the information, i.e. consent or another legal basis

The information types (data fields), how the data will flow and where it will be held, the risks to its security when in transit and at rest, and what will happen once the purpose has been achieved (the information lifecycle).

Design
Once the determination stage is complete and all the relevant information is collated, the design stage incorporates the following:

- Security standards governing the shared information and who will be responsible
- System operation
- Stakeholder/End-user materials

Care should be taken to ensure that information is handled under the Council policy and within the bounds of the relevant laws. The GDPR has 6 Principles to be adhered to.

Section 1 Submitting controller details?

Name of the controller	
The Ivers Parish Council	
Subject and Title of DPO	
CCTV	
Name of controller Contact or DPO	
Gareth Eynon - Satswana Ltd Suite G12, Ferneberga House, Alexandra Road, Farnborough GU14 6DQ	
Date	26/11/2024

Section 2 Identify the need for a DPIA.

Explain broadly what the project aims to achieve and what type of processing it involves. You may refer to other documents, such as a helpful project proposal. Summarise why you identified the need for a DPIA.

What is the aim of the project?

CCTV consistently delivers benefits in terms of improved health and safety and security within Councils. It complements other security measures which are in place within the Council.

CCTV aims to achieve the following:

- To protect staff, volunteers, visitors and members of the public with the regard to their personal safety.
- To protect the Council owned and managed buildings, land and equipment, and the personal property of staff, volunteers, visitors and members of the public.
- To support the police and community in preventing and detecting incidents and assist in the identification and apprehension of offenders.
- To monitor the security and integrity of the Council premises and deliveries and arrivals.
- To monitor staff and contractors for the purposes of Health and Safety.

Section 3 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 referring to a flow diagram or other way of describing data flows helpful. What types of processing identified as likely high-risk are involved?

The Council's CCTV Privacy Notice provides a legitimate basis for collecting staff, volunteers, visitors and members of the public data. This data relates to health and safety and safeguarding vulnerable groups.

How will you collect, use, store and delete data? – The CCTV system will provide the Council with pictures from 13 fixed based cameras located around the perimeter of the pavilions and workshop buildings and the images will be transmitted/captured on a digital video recorder (DVR). The CCTV system is operational 24 hours a day, 7 days a week.

The images are transmitted to a digital video recorder which is housed in a locked cupboard at the premises. Access is restricted via a locked door. Access to the premises is via a secure door entry system. The images are stored on the hard drive of the digital video recorder. The DVR is located within a locked cupboard.

The transmitted images can be viewed live in the locked room on a video screen by the Clerk and Deputy Clerk and via a PC in the Council Offices. This is documented in the CCTV Policy. This helps to maintain site security, access control, citizen and staff safety.

What is the source of the data? – The CCTV system provides still/video pictures, which are transmitted from cameras positioned in various locations around the perimeter of the pavilions and workshop buildings. All of the CCTV cameras are fixed on a particular scene. The location of the CCTV cameras are as follows:

- 13 cameras are located around the perimeter of the pavilions and workshop buildings.

Will you be sharing data with anyone? The information is used to ensure the health and safety and security of staff and visitors. They can be used to detect unauthorised access to Council buildings and protection of damage to Council assets. The information may be shared with Councillors and the Police for investigation and enforcement purposes.

Disclosure of data is covered by the Council's internal processes which are fully compliant with relevant legislation and Codes of Practice (please see the Council's CCTV Policy).

What types of processing identified as likely high-risk are involved? – Recording of images. Storage of images securely. Appropriate data retention applied to the images.

The digital video recorder is located in the locked cupboard. Access to the images is password protected.

Data Management controls include passwords to the CCTV system. (see comment above)

Individuals can request copies of CCTV data which contains their personal information by submitting a Subject Access Request.

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?

What is the nature of the data? The CCTV data captured are still and video recordings.

Special Category data? – By default the CCTV may be picking up special category data including race/ethnic origin and the health of an individual.

How long will you keep the data? Images will be retained for 30 days unless requested as part of an incident and then stored on archive for the period of the investigation process or for 12 months whichever is the lesser. The Data Management System automatically deletes the information after 30 days. This needs to be included in The Council Data Retention Policy. Recommend data retention meets industry standards (28 to 31 days).

Scope of data obtained? – The CCTV images are obtained within the confines of the Council.

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?

Have you signed up for any approved code of conduct or certification scheme (once any have been approved)?

What is the nature of your relationship with individuals? The Council may receive a number of visitors on a daily basis including contractors, inspectors, support and agency staff, etc.

How much control will they have? The Council does inform staff and visitors that CCTV is in use by installing signs detailing their presence. Located in various locations around the Council site. Recommendation that these signs contain details of who the data controller is (i.e. The Ivers Parish Council) and the council's contact telephone number. The CCTV signage needs to be located on entry to the Council site (car park and pedestrian access). It also needs to be located to the rear of the site.

The CCTV system is capable of identifying individuals from the system and the images can be used in both criminal and civil court cases.

If a Subject Access Request is made data may be downloaded or copied for release to the data subject or a third party (in the case of a Data Protection request). Each request for data must be requested via a signed data release form. In the case of the Police this can be authorised by a person at the rank of Sergeant or above using a WA170 form.

Do they include children or other vulnerable groups? Cameras are located in areas where visitors and staff have access. Cameras are not located in areas where privacy is expected. There are no cameras in toilet areas, changing rooms, and there are no cameras aimed at private areas such as residents' houses, etc. CCTV signage is clearly visible.

Are there prior concerns over this type of processing or security flaws? The Council has a CCTV Policy. The system is operated in line with relevant legislation and the Surveillance Camera Code of Practice (consideration respecting data retention). Recommendation is that staff operating/using the system must have undertaken Data Protection and Information Security training

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 CCTV system is proportionate and justified. It also achieves for the council the following benefits:

1. demonstrates a duty of care to its staff, and visitors
2. protects the fabric of the Council both externally and internally
3. as a consequence of this budgets can be reduced/deferred to other council projects
4. encourages improvement visitor/citizen behavior
5. provides assistance in the detection and prevention of crime
6. to assist in managing the council

CCTV system is referenced in the council's Privacy Notice.

Section 4 Consultation process

Consider how to consult with relevant stakeholders:
describe when and how you will seek individuals' views – or justify why it's inappropriate. Who else do you need to be involved with 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 system has 13 cameras. The Council is looking to upgrade its system with additional cameras. The Council will need to consider the CCTV Passport to Compliance guidance prior to implementation.

The decision to install and expand the CCTV system would be agreed by The Council's Councillors.

This will be communicated to staff and visitors via the Council's CCTV Privacy Notice. This will be published on the Council website.

A list of camera locations is included in appendix 1.

Section 5 Assess necessity and proportionality.

Describe compliance and proportionality measures, in particular:
what is your lawful basis for processing? Does the processing 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?

What is the lawful basis for processing? – The lawful basis for processing is contained in the Council's CCTV Privacy Notice. The lawful basis includes the following:

- Article 6 and Article 9 (Special Category Data) under Data Protection Law
- The Common Law Duty of Care
- Health and Safety at Work Act
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)

Does the processing achieve your purpose? – Cameras are located in areas where staff and visitor have access. Cameras are not located in areas where privacy is expected.

Is there another way to achieve the same outcome? – To support Council security a locked in Council policy has been adopted along with improved lighting and other improvements have been put in place.

How will you prevent function creep? – The lawful basis for processing will be contained in the Council's CCTV Privacy Notice. Where there have been material changes to the way CCTV is used, the Council will undertake a review of its CCTV system to ensure compliance and mitigate against 'function creep.'

How will you ensure data quality and data minimisation? – Consider the source of the data. The Council will consider developing a separate data retention policy which identifies data retention periods for CCTV. However, the Council will note data retention periods against CCTV as documented in the Information Asset Register. The Council will continue to be compliant with its CCTV Policy.

What information will you give the individuals? – The Council will inform staff and visitors that CCTV is in use by installing signs detailing the scheme and its purpose, along with a contact telephone number. The Council does have a Privacy Notice for its CCTV.

How will you help them support their rights? – The Council has a Subject Access Request procedure in place to ensure compliance with Data Protection Law. CCTV signage states a contact telephone number. The Council will continue to be compliant with its Data Protection Policy.

Section 6 Identify and assess risks.

Describe the source of risk and the nature of the potential impact on individuals.
Include associated compliance and corporate risks as necessary.

Risk	Likelihood of harm	Severity of harm	Overall risk
Positioning of CCTV cameras at entrance points to the Council and the issue of privacy	Remote	Minimal	Low
Housing of CCTV cameras outside and ingress of water	Possible	Signifcant	Medium
Ongoing maintenance of CCTV equipment preventing breakdowns, etc	Possible	Signifcant	Medium
CCTV policies and procedures not in place leading to inconsistencies, etc	Probable	Severe	Medium
Appropriate CCTV signage in place which conforms to industry standards	Possible	Minimal	Low
Training not undertaken by those using CCTV Privacy (Workforce)	Possible	Signifcant	Medium
Noncompliance when upgrading the Council's CCTV system	Possible	Signifcant	Medium

Section 7 Identify measures to reduce risk.

Describe the source of risk and the nature of the potential impact on individuals.
Include associated compliance and corporate risks as necessary.

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
CCTV & ingress of water	Use of waterproof enclosures.	Reduced	Low	Yes
CCTV Maintenance	Maintenance contract in place with Security Services.	Reduced	Low	Yes
CCTV Policies & Procedures	Policies and Procedures insitu	Reduced	Medium	Yes
Training	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Privacy Notices	Implementing Council data retention periods in the cloud	Reduced	Low	Yes
CCTV Passport to Compliance	Upgrade CCTV using guidance from CCTV Passport to Compliance	Reduced	Low	Yes

Section 8 Sign off and record outcomes.

Item	Name/position/date	Notes
Measures approved by:	Click or tap here to enter text.	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Click or tap here to enter text.	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Choose an item.	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Click or tap here to enter text.		
DPO advice accepted or overruled by:	Choose an item.	If overruled, you must explain your reasons
Comments: Click or tap here to enter text.		
Consultation responses reviewed by:	Click or tap here to enter text.	If your decision departs from individuals' views, you must explain your reasons
Comments: Click or tap here to enter text.		
This DPIA will kept under review by:	Click or tap here to enter text.	The DPO should also review ongoing compliance with DPIA
DPIA next review date:	Click or tap to enter a date.	

Appendix 1

List of Camera Locations

Jubilee Pavilion

1. **Car Park (facing High Street)**
2. **Car Park (facing into recreation ground)**
3. **Car Park (by Workshop Gated Entrance)**
4. **Gated Entrance by Workshop**
5. **Jubilee Pavilion Entrance Door**
6. **Jubilee Pavilion Rear Exit Door**
7. **Jubilee Pavilion Rear External Storage Area**
8. **Jubilee Pavilion Patio**

Iver Heath Pavilion

1. **Car Park**
2. **Car Park (facing entrance from Church Road)**
3. **View to Tractor Shed**
4. **Iver Heath 8Entrance Door**
5. **Tennis Club Entrance Gate**