BERRYFIELDS PARISH COUNCIL
Roman Park Hall, Sir Henry Lee Crescent, Aylesbury HP18 0YT
Telephone: 01296 925750
Email: clerk@berryfieldspc.org

CCTV POLICY

1. Purpose and Scope

1.1 This policy sets out how Berryfields Council (BPC) will operate and maintain the closed-circuit television (CCTV) system at Roman Park Hall.

1.2 CCTV cameras are den Roman Park Hall to:

- Ensure the safety of staff and visitors;
- assist in the maintenance of public order and reduce offences involving vandalism, nuisance and antisocial behaviour;
- deter individuals from damaging property or assist in identifying those who cause damage to property;
- assist in the monitoring, identification, and enforcement of action whereby crime is suspected to have been committed through provision of footage as evidence as applicable; and
- reduce fear of crime or intimidation by individuals or groups by developing a safe and secure environment

1.3 The CCTV system installed at Roman Park Hall will comply with relevant legislation. This policy considers the:

- Surveillance Camera Code of Practice (see Appendix A)
- CCTV Code of Practice issued by the Information Commissioners Office (ICO)
- Requirement for processing personal data as set out in the General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Right to privacy as set out in Article 8 of the Human Rights Act 1998

2. CCTV System within Roman Park Hall

2.1 CCTV cameras have been sited to capture images that are relevant to the specified purpose for which the system has been established. (See 1.2 above)

2.2 CCTV is operated from cameras located on the outside walls, facing the piazza, car park, back yard, side/greenway and side of building. There is also CCTV inside the building, reception area, kitchen and bar.

2.3 Cameras are sited to ensure that they produce images of sufficient quality, ensuring.

consideration for technical and environmental issues.

2.4 The CCTV system will not be used to invade the privacy of any individual and will not. be used for the monitoring of any individual without proper due cause.

2.5 There is audio recording using this system. Signs are displayed in these areas, which includes reception, kitchen and bar. There are no cameras or audio in any of the halls, meeting rooms or toilets.

2.6 CCTV may be subject to live monitoring from the BPC office or remotely.

2.7 Signage will be clearly visible so that the public are aware of the system and will clearly state that the owner of the system is BPC, along with contact details for any further queries.

2.8 BPC will perform a privacy impact assessment when installing or moving CCTV cameras to consider the privacy issues involved when using new surveillance systems.

3. Storage & Retention of CCTV Images

3.1 Recorded information is held on digital recorders or in secure computer files with restricted access.

3.2 Images are recorded and retained for up to 31 days unless they are required for an ongoing investigation.

3.3 Recorded images will be of a high quality, in order for recorded material to be admissible in court.

3.4 Where footage is required for an investigation, a copy will be held for up to one year, or such other period as may be necessary to progress the investigation.

3.5 Images retained for evidential purposes will be retained in a secure place where access is controlled.

4. Access to CCTV Images

4.1 Access to recorded images will be restricted to authorised individuals and will not be made widely available.

4.2 No unauthorised access to the CCTV screens will be permitted at any time.

4.3 Recorded images will only be viewed from the monitoring room or via remote access locations with restricted access.

4.4 At any time whereby the review or monitoring of CCTV footage, live or recorded, is carried out the monitoring room is to be a secure environment. To ensure this, only authorised persons with a legitimate purpose will be permitted access.

4.5 Security measures will be taken to prevent unauthorised access to, alteration, disclosure, destruction, accidental loss or destruction of recorded material.

4.6 All access to CCTV images will be logged in the CCTV Logbook

5. Access to/Disclosure of CCTV Images

5.1 Access or disclosure requests will only be authorised by the Data Controller and must be received within 14 days of the footage being taken. Requests will only be granted if the request falls within the following categories:

- Data Subject (persons whose images have been recorded by the CCTV) – this is dealt with in section 6 below;
- Law enforcement agencies;
- A member of BPC in the investigation of a crime;
- A member of BPC in the investigation of a Health & Safety at Work Act incident;
- Relevant legal representative of data subjects.

5.2 Law enforcement agencies may view or request copies of CCTV images if requested in person and subject to authorisation of the Data Controller.

5.3 To ensure the preservation of images for evidential purposes, the following will apply

- DVD/USBs must be identified by a Name, Date, Time & Camera Location.
- The DVD/USB must be signed by the person who downloaded the images, dated, witnessed and stored in a sealed envelope in BPCs fire safe.
- The log must be completed detailing the release of the DVD/USB to the Police or other agency.
- If a DVD/USB is required as evidence, a copy may be released to the Police who will become the Data Controller and therefore responsible for the images.
- The Police may require BPC to retain stored DVD/USBs for possible future evidence. Such DVD/USBs will be indexed and securely stored in the BPC fire safe for a period of one year, at which point they will be securely destroyed.

6. Subject Access Requests

6.1 The GDPR provides individuals with the right to access a copy of their personal data held by BPC. This includes the right to access a copy of CCTV images. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in the Data Protection Act 2018. They do not have the right to instant access.

6.2 If a request for images is received via a Freedom of Information Act (FOIA) application and the person requesting is the subject, these will be exempt from the FOIA and will be dealt with under the Data Protection Act 2018 and the GDPR (known as Subject Access Requests).

6.3 A person whose image has been recorded and retained and who wishes to access the data must apply in writing to the Parish Clerk within 14 days of the footage being taken. All applications must be made by the Data Subject themselves, or their legal representative. Requests will be processed promptly.

6.4 GDPR allows the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension for prosecution of offenders. If a Data Subject Access request is refused, the response will be fully documented and the Data Subject informed in writing, stating the reasons.

6.5 If images of third parties are also shown with the images of the person who has made the access request, consideration will be given as to whether there is a need to obscure the images of third parties. If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they should be refused.

6.6 BPC as the Data Controller will make the final decision about disclosure.

7. Accountability and Responsibilities

7.1 BPC and the Parish Clerk are responsible for ensuring compliance with the policy in relation to all CCTVs operated by BPC.

7.2 BPC is the Data Controller for the purpose of data protection legislation and is responsible for the security, storage and integrity of data, and the releasing of data to third parties who have a legal right to receive copies of such.

7.3 All users of the CCTV system must act in accordance with this policy and all other associated policies and procedures.

8. Complaints

8.1 A member of the public wishing to make a complaint about the CCTV system may do so through BPC's complaints procedure. A copy of this procedure can be found on www.berryfields-pc.gov.uk

8.2 All complaints should be made in writing to either clerk@berryfieldspc.org or Parish Clerk, Roman Park Hall, Sir Henry Lee Crescent, Aylesbury HP18 0YT.

8.3 A log of the number of complaints and nature of enquiries received will be maintained together with the action taken.

9. Annual Review

9.1 The ICO's CCTV Code of Practice stipulates that the CCTV system should be reviewed annually to determine whether CCTV continues to be justified. It further states that it is necessary to establish the system's effectiveness to ensure that it is continuing to meet the operational requirement. If it does not achieve the purpose for which it was intended, it should be stopped or modified.

9.2 There will be an annual policy review covering the following aspects:

- Any change to validity of operational requirements and objectives.
- changes to the CCTV system.
- review of the Data Protection Act 2018 and legislations associated to the usage of CCTV systems.
- maintenance log and any ongoing and outstanding issues.
- Complaints procedure.
- Identification of trends.

APPENDIX A: Surveillance Camera Code of Practice

The Surveillance Camera Code of Practice was issued in 2013 following the introduction of the Protection of Freedoms Act 2012 and further updated in 2014. The Code provides guidance on the appropriate and effective use of surveillance camera systems.

BPC is a relevant authority as defined by Section 33 of the Protection of Freedoms Act and therefore must have regard to the code.

The code applies to the use of surveillance camera systems that operate in public places, regardless of whether there is any live viewing or recording of images or information or associated data.

The code provides 12 guiding principles which BPC has adopted. These are:

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- The use of a surveillance camera system must consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held, and used.
- Clear rules, policies and procedures must be in place before a surveillance camera system is used and these must be communicated to all who need to comply with them.
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system and such images and information should be deleted once their purposes have been discharged.
- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice and regular reports should be published.
- When the use of a surveillance camera system is in pursuit of a legitimate aim and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
- Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Appendix B: CCTV Camera Location Plan

Reception – with audio

Kitchen – with audio

Bar

Back emergency exit.

Outside area – covering all sides of the building and car park

Please note there are no cameras in either halls or meeting room.

Document History

Approved and adopted	01/01/2022	(version 1)
Reviewed by Parish Council	17/02/2024	(version 1)